JULY/AUGUST 2021

intercom

THE MAGAZINE OF THE SOCIETY FOR TECHNICAL COMMUNICATION

CYBERSECURITY

BEST PRACTICES, INDUSTRY SHIFTS, AND CAREER OPPORTUNITIES FOR TECHNICAL COMMUNICATORS

6 The Importance of Technical Communication in Cybersecurity

12 Where Cybersecurity and Technical Communication Intersect

18 A Cybersecurity Quick Start Guide

24 Developing Engaging Cybersecurity Training

29 Breaking Down Cybersecurity into Its Essential Components

34 Compliance Careers for Technical Communicators

38 Cybersecurity and Documentation

44 A Security Awareness Professional's Perspective in Higher Education

48 A Short Career Sojourn into Cybersecurity

July/August 2021

Volume 68 | Issue 4

2 **From the Editor**
By Alisa Bonsignore

3 **From the Guest Editors**
By Dr. Jackie Damrau and Ben Woelk

FEATURES

6 **Technical Communication & Cybersecurity**
By Adam Coreil
"It's not what you say, it's how you say it." Explore the principals of clear, universal communication and its unique challenges within cybersecurity.

12 **At the Intersection of Cybersecurity and Technical Communication: Cybersecurity Frameworks Provide Opportunities for Technical Communicators**
By Dawnell Claessen, CISSP
Investigate the frameworks that govern cybersecurity, the technical communicator's role in establishing and adhering to guidelines, and the possibility as a logical career progression.

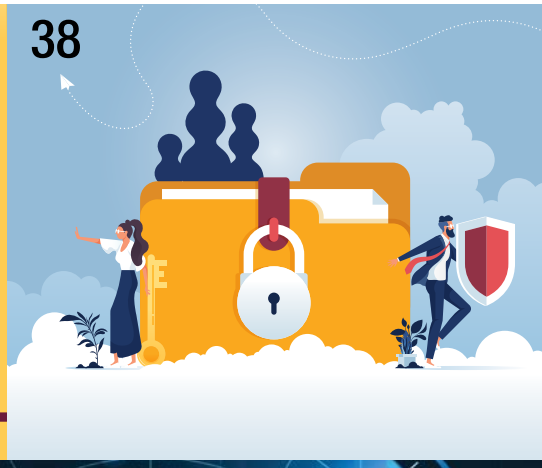
18 **How to Cyber: A Cybersecurity Quick Start Guide**
By Jessica Behles
The author provides a basic introduction to cybersecurity and important cybersecurity terms.

24 **Developing Engaging Cybersecurity Training**
By Liz Herman
Traditional corporate cybersecurity training often leaves employees bored and disengaged—but can technical communicators find ways to make training effective and engaging?

29 **Beyond the Weakest Link: Maturing End User Information Security Education to Bolster Organizational Defenses**
By Valerie Vogel and Joanna Grama
Break down cybersecurity into its essential components: people, processes, and technology.

34 **Compliance Careers for Technical Communicators**
By Kat Reierson
If you enjoy documenting processes and researching rules and regulations, then a career in compliance writing may be for you!

38 **Cybersecurity and Documentation: Security Considerations for Authors**
By Bridget Khursheed
Examining the best practices, risks, solutions, and mitigations that technical communicators can put in place now to protect their companies, teams, and themselves.



44 A Great Adventure: Working as a Security Awareness Professional in Higher Education
By Ben Woelk
Woelk looks back on his 17 years at the Rochester Institute of Technology and what it takes to be in the cybersecurity field in a higher education setting.

48 A Short Career Sojourn into Cybersecurity
By Dr. Jackie Damrau
Dr. Damrau shares her journey moving from a senior business analyst into a senior risk analyst/project manager for a global commercial real estate company.

SOCIETY PAGES

52 TC Authors Honored at 2021 CCCC Technical and Scientific Communication Awards

53 Searching for Your Next Tech Comm Dream Job?

53 Technical Communication Academic Resources: The Academic Database

53 Upcoming Online Courses

54 Get Certified!

COLUMNS

MEET THE CHANGE AGENTS

55 Helping Eli Lilly Move to Adopt Structured Content for Customer Experience Improvements and Future Automation
By Scott Abel

CONTENT ENGINEERING

58 The Hidden Information Security Killers Hiding in Content, Metadata, and Operations
By Cruce Saunders

THE ACADEMIC CONVERSATION

60 When Information Isn't Enough: Cybersecurity Scholarship and the Human Factor
By thomas barker

DEPARTMENTS

OFF HOURS

64 Empowering Women Through Fiction
By Shawneda Crout

intercom

Intercom, the magazine of the Society for Technical Communication, is published to provide practical examples and applications of technical communication that will promote its readers' professional development.

Publisher Society for Technical Communication
Chief Executive Officer Elizabeth E. (Liz) Pohland
Executive Editor Alisa Bonsignore
Editor Lisa Howard-Fusco
Designer Amy Hall

CONTRIBUTING EDITORS
Scott Abel, *Meet the Change Agents*
Thomas Barker, *The Academic Conversation*
Kit Brown-Hoekstra and Cindy Currie, *Ask a Tech Comm Manager*
Cruce Saunders, *Content Engineering*
Ryan Weber, *Student Perspectives*
Russell Willerton, *Ethics*

STC BOARD OF DIRECTORS
Officers
Kirsty Taylor, *President*
Aiessa Moyna, *Vice President*
Craig Baehr, *Immediate Past President*
Bobbi Werner, *Treasurer*
Timothy Esposito, *Secretary*
Directors Todd DeLuca, Laura Palmer, Sree Pattabiraman, Ann Marie Queeney

EDITORIAL ADVISORY COMMITTEE
Kit Brown-Hoekstra, Chair
Saul Carliner
Michelle Corbin
Alyssa Fox
Michael Opsteegh

SOCIETY FOR TECHNICAL COMMUNICATION
3251 Old Lee Highway, Suite 406
Fairfax, VA 22030
+1(703) 522-4114 | +1(703) 522-2075 fax
Send questions and correspondence to the editor at the above address. General information about STC: stc@stc.org *or* www.stc.org.

Address Changes: membership@stc.org
Intercom Editorial: intercom-editor@stc.org

Reprint Permissions: www.copyright.com
Intercom (ISSN 0164-6206) is published 6 times a year by the Society for Technical Communication, 3251 Old Lee Highway, Suite 406, Fairfax, VA 22030, a nonprofit educational organization, as a service to its membership. Membership in STC includes an online subscription to **Intercom**. Periodicals postage paid at Fairfax, VA, and additional offices.
Postmaster Send address changes to **Intercom**, Attn: Membership, c/o Society for Technical Communication, 3251 Old Lee Highway, Suite 406, Fairfax, VA 22030.
Copyright © 2021 by the Society for Technical Communication. All rights reserved. Printed in the USA. All articles in **Intercom** are copyrighted by the authors unless otherwise indicated. Anyone interested in reprints, reproductions, or reuse must contact the authors for permission. To advertise in **Intercom**, contact *intercom@stc.org*, Society for Technical Communication, 3251 Old Lee Highway, Suite 406, Fairfax, VA 22030. Ph: +1(703) 522-4114.

A Note from the Editor

I WAS THRILLED to learn that Dr. Jackie Damrau and Ben Woelk were interested in guest editing an issue about cybersecurity. I spent several years in the industry, and I'm pleased to see how much security awareness is expanding out into other aspects of business.

It's amazing to see how much the industry has shifted in the past two decades. When I first went to work for McAfee, we talked about the vulnerability of data sitting on the hard drives of individual laptops. In February 2020 at the RSA Conference in San Francisco, Juniper Networks estimated that this year, 83 percent of enterprise workloads would be cloud-based. I suspect that the number turned out to be even higher after a year of remote work. That's a lot of content to secure, and it's making cybersecurity a hotter industry than ever.

In their article, "Beyond the Weakest Link," (page 29), Valerie Vogel and Joanna Grama talk about how this sudden shift has caused the security industry to drastically reconsider how we talk about information security practices. "[It] has heightened the need to make sure that users are informed about and empowered to implement information security practices in their remote working environments because technical controls can't always work in an environment not managed by a central IT organization."

But how can we educate people on best practices in ways that truly resonate? In a survey conducted by Dr. Liz Herman, one respondent noted that the current pandemic can and should reshape cybersecurity training. "Show how it impacts people at home as well as work. That way they can have good habits that carry back." You can read more about it in "Developing Engaging Security Training" on page 24.

I hope that this issue gives you new ideas for how to include cybersecurity best practices in your content development. If there are other industries that you'd like us to profile in *Intercom*, send me a message at intercom-editor@stc.org. I look forward to hearing from you.

Alisa Bonsignore
(she/her)

GUEST EDITORIAL

Cybersecurity & Technical Communication: A New Field to Consider

BY DR. JACKIE DAMRAU | *STC Fellow* and **BEN WOELK** | *STC Associate Fellow & Past President, STC*

A NEW FIELD for technical communication professionals to investigate is that of cybersecurity. Just the word itself can cause some to think hard as well as to question: Is it cyber security or cybersecurity? We're not sure that there's a true distinction, but it does mean protecting a company or an individual's information from the bad actors gaining momentum over you and your identity.

A few of our STC members have been in this field for some time; others are new to it. Ben and I proposed this special issue to share with you this field and what it takes to enter it. It's not as difficult as one would think. Those in a company setting have been or should have been exposed annually to cybersecurity training of some type. For those that are independent consultants or freelancers, perhaps not as much—yet you should be aware of how any information you put out can be misused by the bad actors.

We have selected authors that are well-rounded within the cybersecurity field to present you with articles that cover the basic cybersecurity fundamental and the training one needs to consider. They conclude with how and what it takes to work in the cybersecurity field.

In This Issue

In the area of cybersecurity fundamentals:

- In "Technical Communication & Cybersecurity," invited author Adam Coreil covers the universal principles that it takes to communicate effectively (regardless of audience or subject), why there is a need for cybersecurity, and the challenges within it.
- In "At the Intersection of Cybersecurity and Technical Communication: Frameworks Hold Opportunity for Technical Communicators," Dawnell Claessen, CISSP and STC senior member, investigates the frameworks that govern cybersecurity as pathways that use a technical communicator's abilities to establish and adhere to guidelines and standards as a logical career progression.
- As an introduction to cybersecurity, Jessica Behles ("How to Cyber: A Cybersecurity Quick Start Guide") describes how cybersecurity should be a "priority for anyone using internet-connected technology." She describes how to enter the field, and how she created a quick start guide to help her. In this article, Jessica defines many of the introductory cybersecurity terms which one should become familiar with.

Leaving the introduction phase, we go into training within cybersecurity. Here we have:

- Liz Herman's "Developing Engaging Cybersecurity Training," where the basis of her article comes from interviews with two experienced training managers and a social media survey that she conducted to collect additional perspectives. This article reviews cybersecurity training from a general to a narrower focus. The survey results show a diversity of opinions about corporate training on cybersecurity to individual thoughts on how companies should reconsider the type of cybersecurity training they engage in to ensure that the employees are not just breezing through the content to satisfy an annual corporate training goal.
- Rounding out this section is, "Beyond the Weakest Link: Maturing End User Information Security Education to Bolster Organizational Defenses." Authors Valerie Vogel and Joanna Gram, share their perspective on cybersecurity as being broken into essential components of people, processes, and technology (a standard technology discipline). They cover the aspects of a company's information security program: what it is, what it is not, how to "approach information security more strategically by focusing on the people and human risks."

The final section in this special issue shares experiences of how these technical communication professionals became involved in the cybersecurity field. Of course, all our invited authors came into this field from other careers and have shared bits of that in their articles. The goal here is to share the journey taken to break into the cybersecurity field with you, our readers.

- Kat Reierson shares in "Intersection of Technical Communication & Cybersecurity" what it takes to consider a career in compliance. Compliance is more than just documenting processes and knowing the rules and regulations for a specific industry. She says technical communicators are unique in that we have the technical skills to work with SMEs; see what others do not; understand working with policies, procedures, and standards; and can train others on these topics. Kat shared examples of job titles and skill requirements, to see where your skills might lead you into a different career path.

- "Cybersecurity & Documentation: Security Considerations for Authors" by Bridget Khursheed examines the best practices, risks, solutions, and mitigations that technical communicators can put in place now to protect their companies, teams, and themselves. Her article comes from a TCUK 2018 presentation that Bridget has updated to include the latest information. This article also includes perspectives on how companies view security and why your APIs and documents may already be targeted by the bad actors.
- Ben Woelk's "A Great Adventure: Working as a Security Awareness Professional in Higher Education" looks back on his 17 years of work at the Rochester Institute of Technology in the Information Security Office. He has taken his techcomm skill set, applied it to his daily work in cybersecurity, and spends much of his time in cybersecurity training and awareness. Ben takes you on his journey and shares the skills he acquired, the impact he has with and receives from teaching, and what it takes to be in the cyber security field in a higher education setting.
- In "A Short Career Sojourn into Cybersecurity," Dr. Jackie Damrau shares her short journey in this field moving from a role as a senior business analyst into a senior risk analyst/project manager for a global commercial real estate company. During her time, she spent hours researching and reading various regulations and standards, eliciting information from her peers and managers, and continuously absorbing all she could. Her journey interestingly was cut short due to COVID-19 staff reductions; however, her experience has opened her eyes into the world of protecting an individual's and/or company's information in a world of bad actors wanting to take your personal or corporate identity.

Thank Yous

This guest-edited issue would not have been possible without the support of Ben Woelk. Jackie reached out to Ben with her thoughts of wanting to do this issue as they were both in the cybersecurity field at the time. Ben still is in this field and is a consummate professional. Many of the invited authors were recommended by Ben.

Together, we have strived to bring you into the world of cybersecurity by sharing how you can enter this field, what you need to know, the training or certifications you can achieve, and our own personal journeys, to show the possibilities.

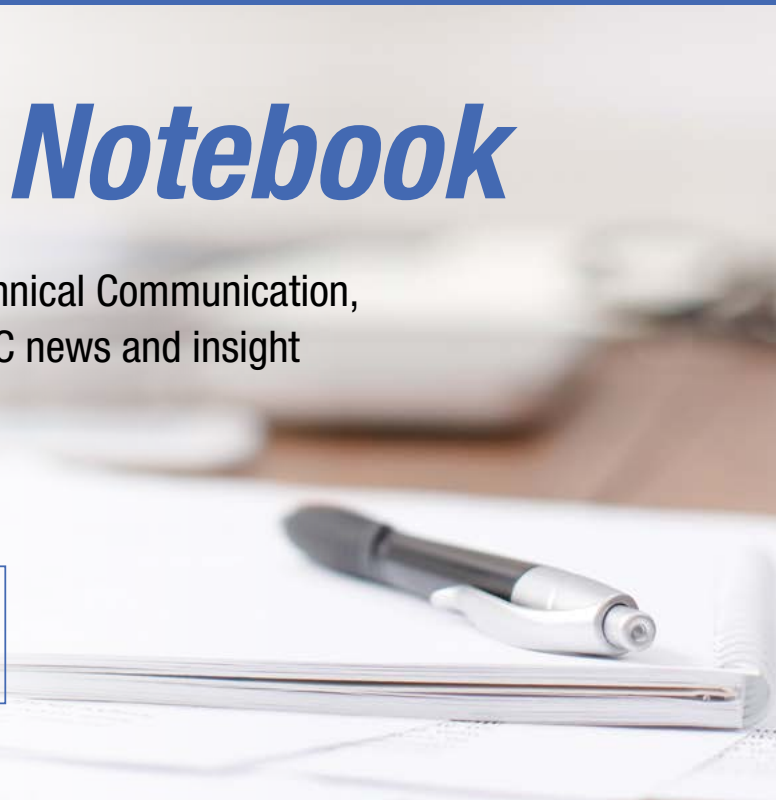
Enjoy this issue! Reach out to Ben and me as we'd love to know your thoughts on the world of cybersecurity.

Read *STC's Notebook*

The official blog of the Society for Technical Communication, *STC's Notebook,* is your source for STC news and insight from the STC community.

Visit *www.stc.org/notebook*

Contribute to the *Notebook!*
Send your submissions to *publications@stc.org*.



Expand your knowledge and enhance your education with

STC Live Webinars

Technical communicators looking for education where they are will find a range of options with STC live Webinars. Topics range from skill development to leadership, management, technology, content and business strategy, and so much more.

STC live Webinars provide two (2) CEUs toward the continuing education requirement for CPTC.

See the full calendar at ***www.stc.org/live-webinars.***

For general inquiries, interest in presenting a webinar with STC, and questions about registration and payment, please contact us at ***education@stc.org.***

Technical Communication & CYBERSECURITY

By ADAM COREIL

MY PARENTS ALWAYS told me, "It's not what you say, it's how you say it," and "Mean what you say and say what you mean." These are universal principles to communicate effectively, regardless of audience or subject. These concepts apply in cybersecurity and in communicating effectively, succinctly, and in the most impactful way. However, communication around cybersecurity issues can be challenging.

Why is there a Need for Cybersecurity Technical Communicators?

Among many, many things that occurred during the unprecedented year that was 2020 (only last year!), organizations across the world were breached by the SolarWinds cyberattack. Over 18,000 of the 300,000-plus SolarWinds customers of network software were affected, including the United States (U.S.) Treasury and U.S. Commerce Department, National Institute of Health, State Department, and Department of Homeland Security, as of the writing of this article (Jankowicz and Davis, 2020). The need for organizations to clearly communicate cybersecurity threats, analyses, and cybersecurity concepts in a meaningful way is critical, now more than ever, to facilitate knowledge sharing across industries, governments, and borders.

Challenges

Cybersecurity departments have consistently struggled to concisely and effectively communicate cybersecurity risks, standards, and guidance. This inability has led to confusion, inconsistent security practices, and varying levels of cyber risk management. This phenomenon is not due to lack of cyber global standards and regulations! These standards and regulations include, and are not limited to, the list in Table 1.

Cybersecurity-focused technical communicators have a distinctive opportunity to bridge the communication gap in the following ways:

- Enabling consistent application of security requirements
- Providing documentation that supports treatment of cyber risks
- Authoring support procedures for security operations

Increasingly, cybersecurity is the topic of corporate board meetings and committee focus areas. Demand for clear security awareness and education is key to inform users across the enterprise. Since the COVID-19 pandemic began in 2020, one side effect has been an increase in breaches and hacks from mobile and internet of things (IOT) devices such as household appliances and company devices, including sensors for manufacturing, energy generation, and distribution systems (Sobers, 2021). Additionally, increasing data privacy and protection requirements further necessitate expertise of technical communicators focused on cybersecurity compliance requirements. According to Rob Sobers, a software engineer specializing in web security at Varonis, 95% of cybersecurity breaches are caused by human error. Technical communication professionals who focus on cybersecurity initiatives—projects, processes, and compliance—can add needed clarity to cybersecurity documentation and communications, discussed in the next section.

Cybersecurity departments have consistently struggled to concisely and effectively communicate cybersecurity risks, standards, and guidance.

Security Standards and Procedures

Operational security policies and procedures must be meaningful, easy to understand, and useful for an organization to operate. Security standards must be documented and regularly updated across the organization's technology infrastructure to ensure compliance to laws and regulations. Table 2

Security Framework	Description
National Institute of Standards and Technology (NIST) Cybersecurity Framework	Cybersecurity framework with five core areas: Identify, Protect, Detect, Respond, Recover (U.S. Department of Commerce, 2020). Both government and publicly-traded organizations follow this framework in their cybersecurity function.
Cloud Security Alliance (CSA) Cloud Controls Matrix	Framework of security controls for cloud computing environments that map to other frameworks such as NIST, Payment Card Industry Data Security Standards (Payment Card Industry Data Security Standards, 2021).
ISO 27001 Information Security Management (ISM)	International framework providing requirements for an information security management system (ISMS), enabling organizations to manage financial information, intellectual property, employee details or information entrusted by third parties (ISO Information Security Management, 2021).
Control Objectives for Information and Related Technology (COBIT)	Technology management framework by the Information Systems and Control Association (ISACA) to help businesses implement robust and controlled information management and governance strategies.

Table 1. A list of cybersecurity frameworks

Area	Law or Regulation	Why Is Engaging a Cybersecurity Technical Communicator a Good Idea?
Payment Processing	Payment Card Industry Data Security Standards (PCI DSS)	There are 12 requirements of PCI compliance that are a mix of operational and technical. For a company to transact using credit cards, customer data security must be upheld. The PCI DSS requirements are: 1. Firewall configurations 2. Password management 3. Data-at-rest security 4. Data-in-transit security 5. Up-to-date antivirus 6. Secure system and application development 7. Restricted access to cardholder data 8. Logical access and authentication mechanisms 9. Physical access mechanisms 10. Monitor data access 11. Regularly test security systems and processes 12. Up-to-date information security policy Cybersecurity-focused communicators have an opportunity to ensure operational and technical components of PCI DSS are incorporated into support procedures, process descriptions, and standards for the twelve requirements (Payment Card Industry Data Security Standards, 2021).
Data Privacy	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	The rule's objective is to protect our healthcare information while also allowing the flow of information to support the quality of healthcare and support processes. Organizations that are required to comply would benefit from employing a cybersecurity technical communicator to ensure that system features that transmit, transact, and manage such data have documentation that articulates security features and are embedded to protect in scope healthcare data (Summary of the HIPAA Privacy Rule, 2021).
Information Security	Federal Information Security Modernization Act (FISMA)	Originally enacted in 2002, FISMA was updated in 2014 to address information security risks and focuses on security incidents of federal agencies including (NIST, 2020): • Preparing for security • Risk-based security roles and responsibilities • Security controls periodic reviews • System processing authorization The need to have support documentation for applicable systems should be consistently communicated in processes, standards, and guidelines, which is what a technical communicator would assist in doing.

Table 2. Cybersecurity areas where mature security documentation could add value to compliance efforts

outlines cybersecurity areas where mature security documentation could add value to compliance efforts.

Cyber Education and Security Awareness

Effective security awareness communication must be consistent and easily digestible to equip employees to make good cybersecurity choices; technical communicators are the key to this form of clear communication. According to Allison Johnson, CISO at XEROX (Sparapani, 2017), security departments need to speak in risk terms across the enterprise. One way organizations can achieve effective security and risk communication is through a strong technical communicator who has the capability to bridge technical security and business needs. Because attackers often use social engineering techniques to gain access to protected corporate information, effective security awareness training is a critical success factor. According to the 2020 Verizon Data Breach Investigations Report, cyberattackers are becoming "increasingly efficient and lean more toward attacks such as phishing." This is a type of social engineering that uses malicious emails designed to confuse the target user and creates a sense of urgency to get them to act by opening a malicious attachment, clicking on a link, or take a more egregious action such as changing payment to a customer or vendor. Nearly 40% of malware incidents in 2020 were from email with an embedded link or attachment, according to Verizon.

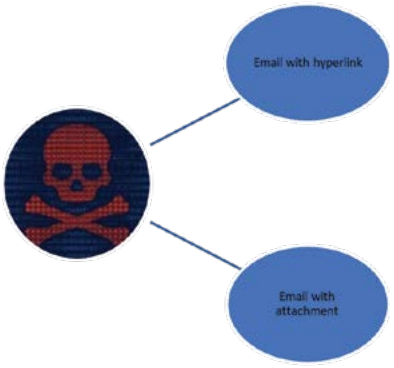


Figure 1. Malicious email components

Application Development: Cybersecurity in the Design

Application development teams are tasked with creating applications that enable business needs. Technical communicators can effectively translate those needs into clearly documented requirements and design

specifications. Moreover, technical communicators who focus on cybersecurity and who participate on product development teams have an opportunity to ensure that product development teams incorporate cybersecurity controls throughout product development.

Although *development operations* (*DevOps*) and *development security operations* (*DevSecOps*) are relatively new terms, they are the practices of bringing together the disciplines of development, operations, and security in a more collaborative, consistent manner. The effect of good DevOps and DevSecOps in application development is shorter development iterations, along with improved flexibility, efficiency, and competitive edge (OpenSource, 2021). Agility and flexibility in today's development practices are key to meeting the demands of business goals and customer outcomes. Application design and functional documentation approaches must also shift to approaches that are flexible to keep pace with DevOps and SecDevOps.

Table 3 outlines the traditional technical communicator role in a traditional support role versus a cybersecurity-centric role.

Summary

Communication and documentation accuracy, clarity, and completeness are essential for good cybersecurity. As this article outlined, the need for expertise in cybersecurity threats, control frameworks, and regulations are vital for organizations to maintain effectiveness of application documentation, meaningful educational awareness communications, and sound practical understanding of cybersecurity practices and compliance regulations. The need for cybersecurity technical communicators will continue to grow as long as humans continue to be the biggest cyber risk.

ADAM COREIL *(adam.coreil@cbre.com) is a cybersecurity professional with more than 20 years' experience in technology governance and risk. He is a Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM). Adam began his career in risk consulting at Deloitte where he gained cross-industry experience in technology solutions. Outside of work, Adam enjoys research, running, and time with family.*

Technical Communicator Roles Comparison: Traditional Support Role vs. Cybersecurity-Focused DevOps Role		
Focus Area	**Traditional Technical Communicator Role**	**Cybersecurity-Focused Technical Communicator DevOps Role**
Commitment	As required involvement; pre-release phase	Dedicated participation throughout the development process
Concern	Priority on functional features	Security features equally important as functional features
Challenge	Uninvolved in the testing process	Hands-on experience with application development and sandbox testing

Table 3. Comparison of technical communicator roles, traditional support vs. cyber-centric

REFERENCES

International Organization for Standardization. 2021. "ISO Information Security Management." Accessed 21 May 2021. *https://www.iso.org/isoiec-27001-information-security.html.*

Jankowicz, Mia, and Davis, Charles. 2020. "These Big Firms and U.S. Agencies All Use Software from the Company Breached in a Massive Hack Being Blamed on Russia." *Business Insider.* Accessed 21 May 2021. *https://www.businessinsider.com/list-of-companies-agencies-at-risk-after-solarwinds-hack-2020-12.*

NIST. 2020. "NIST Risk Management Framework." Accessed 21 May 2021. *https://csrc.nist.gov/projects/risk-management/detailed-overview.*

OpenSource. 2021. "What is DevOps?" Accessed 21 May 2021. *https://opensource.com/resources/devops?intcmp=7013a00000263HlAAI.*

PCI Security Standards Council. 2021. "Payment Card Industry Data Security Standards." Accessed 21 May 2021. *https://www.pcisecuritystandards.org.*

Sobers, Rob. 2021. "134 Cybersecurity Statistics and Trends for 2021." Varonis. Accessed 21 May 2021. *https://www.varonis.com/blog/cybersecurity-statistics/.*

Sparapani, Jason. 2017. "Xerox CISO: Cybersecurity is 'Enabler' For Innovative Tech." *TechTarget.* Accessed 21 May 2021. *https://searchcio.techtarget.com/video/Xerox-CISO-Cybersecurity-is-enabler-for-innovative-tech?_gl=1*cazgl*_ga*MTEzMjQ2Mzc2OS4xNjEzODU2MDMz*_ga_RRBYR9CGB9*MTYx-Mzg1NjAzMi4xLjAuMTYxMzg1NjAzMi4w&_ga=2.181279588.233816123.1613856033-1132463769.1613856033.*

U.S. Department of Health & Human Services. 2021. "Summary of the HIPAA Privacy Rule." Accessed 21 May 2021. *https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html#:~:text=The%20Privacy%20Rule%20protects%20all,health%20information%20(PHI).%22.*

U.S. Department of Commerce. 2020. National Institute of Standards & Technology Cybersecurity Framework. Accessed 21 May 2021. *https://www.nist.gov/cyberframework.*

UNITE YOUR TECH COMM TEAM WITH

STC's Corporate Value Program

Corporate Value Program (CVP) membership enables organizations to purchase a package of individual memberships for your entire tech comm team, at an overall discounted rate. Companies are eligible to join as a CVP member with a team of five or more technical communicators. When your company invests in a CVP membership, each employee enrolled receives industry tips, tool trainings, professional development, networking opportunities, and other high-quality resources. It's a win-win for your company and your entire team!

Ready to enroll?

Complete the online application at **www.stc.org/membership/corporate-value-program**

Perks of all CVP memberships:

- No new member enrollment fee
- Memberships are transferable to new employees when one leaves your company
- Discounted job posting rates on STC's Job Bank: For a 10% discount, use the code: STCCVP
- Opportunity to sponsor a member-only live webinar (additional costs may be involved)
- Opportunity to participate as a presenter in STC's Technical Communication Summit conference sessions, or as a contributor in STC's Notebook blog and *Intercom* magazine articles
- Discounted rates on advertising, email blasts, and exhibit space at STC's Annual Conference
- Buy five live webinars for company employees and receive the sixth for free.

AT THE INTERSECTION of Cybersecurity and Technical Communication:

Cybersecurity Frameworks Provide Opportunities for Technical Communicators

By DAWNELL CLAESSEN | *STC Senior Member*

TECHNICAL COMMUNICATORS LOOKING to expand their area of practice into cybersecurity should consider frameworks as a pathway that will have many familiar skill sets, work products, and methods. In technical communication (TC) we are well accustomed to establishing and adhering to guidelines and standards, so conducting our work inside a frame of reference (like a framework) should be an easy and logical career step.

What Is a Framework, Anyway?

A *framework* is a tailored set of standards and rules that can be used to form a persistent and reusable infrastructure that organizations use to conduct operations. Frameworks can be as rigid or flexible as an organization needs and are used to execute strategy and meet goals and objectives. Frameworks are also commonly used to assess or demonstrate compliance with specific regulations.

Frameworks are a versatile tool and can be applied as a business model that could be used for research and development of just about anything imaginable. Coding and programming are most often done using a framework of some sort for consistency. Because frameworks allow for a consistent process execution, they can make repeatable processes easier and make both compliance assessment and demonstration more successful. Increasingly, businesses and organizations are relying on frameworks for cybersecurity and TC to fulfill a large and vital part in their use.

A *security framework* is the system of security specific guidelines, policies, regulations, and standards an organization adheres to in achieving its security objectives. This may include physical security, personnel security, as well as security of information, systems, and intellectual property.

A *cybersecurity framework* then is the set of core functions that an organization specifically identifies and performs concurrently and continuously according to set guidelines and standards to achieve its cybersecurity objectives. Often those objectives include things like risk management and/or compliance with regulation.

Figure 1. Technical communication and cybersecurity word cloud

Dozens of cybersecurity frameworks are in use worldwide. One of the most common cybersecurity frameworks in the United States (U.S.) is the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF). The NIST RMF has components, tiers, attributes, and functions. The core functions of this framework are: Identify, Protect, Detect, Respond and Recover (Figure 2). Each core function of most cybersecurity frameworks has a set of controls, including the NIST framework. Each control has implementation guidance and assessment procedures.

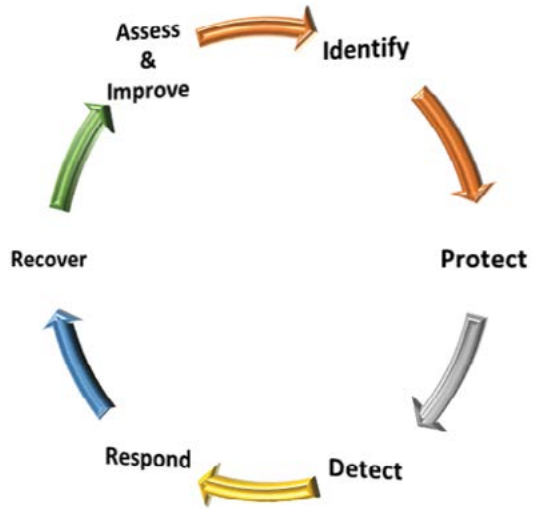


Figure 2. NIST RMF core functions

ISO IEC 27001/ISO 27002 and the ISO 27001 cybersecurity frameworks contain international standards with both having recommendations on a set of requirements and controls. The General Data Protection Regulation (GDPR) is common in Europe, including many industry-specific frameworks like health care, payment cards, manufacturing, etc. Most U.S. frameworks are voluntary, but international frameworks are linked even more closely to compliance with regulations and standards. In other parts of the world, the use of frameworks may be a requirement for certain business types like in Europe with businesses in the payment banking and finance areas.

All frameworks can be tailored and should be used to assess adherence to standards and to improve upon the processes it contains. Choosing an established cybersecurity framework for your organization provides many advantages, like pre-written requirements, taxonomies, standard artifacts, and even templates to make getting started easier.

Cybersecurity Capability Maturity Model (C2M2)

The C2M2 is a maturity model that organizations can use to measure the maturity of their cybersecurity

capabilities. This is typically implemented when an organization wishes to demonstrate or prove that their cybersecurity processes are performed at a certain level of maturity. For example, some contracts that have cybersecurity responsibilities require that bidders be performing at a certain level to even be considered.

There are 10 domains in the model (which is also considered a framework) and each domain has practices and at least three maturity levels. Often these practices are related to management functions, such as risk management, identity and access management, configuration management, supply chain management, and other specific cybersecurity objectives.

Opportunities for Technical Communicators

Technical Communicators are excellent candidates for a career in cybersecurity and especially for working with frameworks. We already know our audience and we know a lot about our organization's people, products, and processes. And we excel at using technology to create and share our knowledge and skills. Automation tools as well play key roles in frameworks. TCs can synthesize all these elements into content that is readable and supports cybersecurity efforts.

Frameworks often come with built-in templates that can be implemented immediately and serve as starting points for developing a library of required process documents. Business processes within your own organization are likely to be linked to a framework of some sort, and they are an accessible and excellent way to get involved with frameworks.

The Art of Artifact Creation and Maintenance

Compliance to a framework of standards and guidelines and their associated policies and procedures is / should be "artifact-centric" by design. TCs are (or can quickly become) experts at "compliance by design" with an artifact-centric approach to writing. All that means is that inception processes are modeled and procedures are written in a more declarative manner (with the goal of compliance and artifacts) versus the imperative (a sequence of steps and actions). This style of writing is what we as TCs would have little trouble implementing.

Artifacts should be a natural work product of any framework. This is the area where TCs can really bring value to the team. As with any form of compliance, an organization must always "say what we do" (follow the process), "do what we say" (generate quality artifacts and records), and "prove it and improve it" (assess, audit, and act on discrepancies).

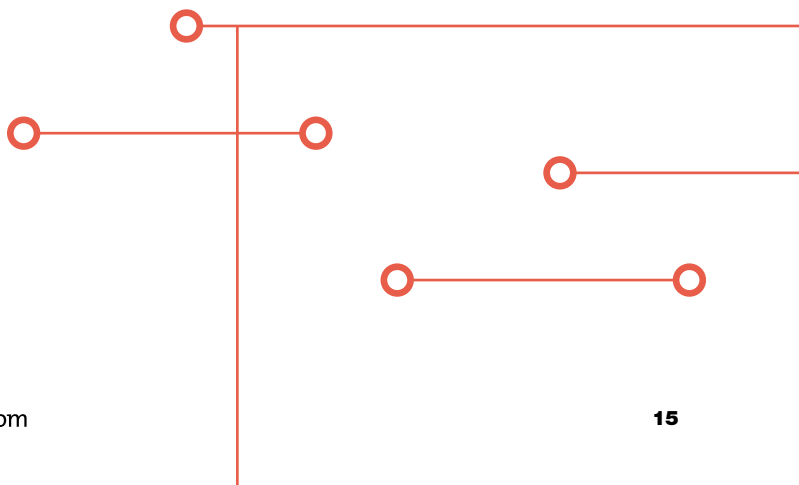
Many cybersecurity frameworks come with a set of standard artifacts and deliverables that typically start with a security plan that addresses all requirements, at least at a high level. Often there are plans subordinate to the main security plan. There are also process documents, requirements and controls, as well as formal reports, lots of metrics to track, and presentations that also present opportunities for TCs to show off their skills.

Getting Started

The news is filled with reports of unfilled cybersecurity jobs—*Forbes* magazine and Cybersecurity Ventures estimate as many as 3.5 million jobs globally by the end of 2021. So, the opportunities exist, and not just for those with hard technical skills and computer science degrees. Frameworks especially rely on communication—good planning and good documentation that is available and accessible to everyone in the organization. Good communication skills are always expected to round out a skill set and should always be highlighted on a résumé. Project management skills are also in remarkably high demand in cybersecurity and framework positions.

There are several ways to get started. First, determine if cybersecurity and frameworks is a good fit for your skill set and career goals. If you think it is, be flexible and know you can always grow your skill set—"upskilling" and "reskilling" is common in cybersecurity so you will constantly be sharpening your non-technical communication skill set. Frameworks are constantly evolving and maturing to match regulations and standards. The ability to learn new things—new technology, new regulations, and standards, all the while using a basic skill will be key to success in cybersecurity.

You can also find opportunities by simply browsing the many job postings online that contain the words cybersecurity + frameworks. Look at the job descriptions and skills noted in the posting and consider what interests you. Writing or technical communication may not be mentioned, so look for terms like policy, process, procedures, assessment, compliance, reports, and artifacts. Look within your company for areas in your current organization that have openings or just need your help. That can be as a job seeker, a consultant, or within your current organization. You can also work with online recruiters and temporary placement agencies. And you can always just decide to go for it! Then, make a career transition plan and do whatever it takes to set yourself up to succeed.



Tools and Techniques

Frameworks are often implemented through technology. The key to success is being able to use these tools. For example, process tools which enforce an automated compliant workflow. Power Automate and SharePoint are very commonly used, but there are many others. Skills with word processing and spreadsheets is an absolute must. Again, our good communication skills come in handy. The use of presentation software and good speaking and presenting skills are always valued.

After communications skills, being able to quickly adapt, to pick up and use new tools and techniques will always serve TCs well and set us apart in the cybersecurity field.

Role of Certifications

In technical communication and cybersecurity, a certification demonstrates a certain level of competency as well as a commitment to the field of practice. This is especially true in cybersecurity where they are quite common. A certification can open doors in cybersecurity

and frameworks and lead to advancement opportunities. If there is a certification that is common in your industry or at your workplace, preparing for a new certification is a way to signal interest and get noticed. Many jobs require or strongly prefer a four-year college degree. But for those who have not completed a bachelor's degree, one or more certifications can help with getting started and advancing in cybersecurity and frameworks.

There are many certifications to consider but one option is to first obtain a Certified Professional Technical Communicator (CPTC) certification and then add a hard skills certification and possibly a project management certification. A certification that is specific to an industry is likely to be extremely helpful in that field but does limit your options a bit.

Consider a certification in a "hard-skill" and choose one you already know, or one that is in demand and technology specific, such as Cisco for computer networking, VMWare for virtualization, Microsoft for Systems Administration, Amazon Cloud, and many others. Spend time browsing job postings and job descriptions of positions and make notes of which ones are mentioned the most. Then consider those that are the best fit for you.

There are many certifications to consider. Here is a list of a few well-known certifications—a quick search online should yield details about each one.

- STC's Certified Professional Technical Communicator (CPTC)
- Information Technology Infrastructure Library (ITIL): Numerous certification offerings with levels of advancement and many specific to process. Very desirable with levels of advancement.
- OCEG's Governance Risk and Compliance Professional (GRCP) and GRCA (Audit)
- PMI's Project Management Professional (PMP)
- CompTIA: Multiple cybersecurity and technical certifications along a career advancement path
- ISACA's Certified Information Systems Auditor
- ISC(2): CISSP and others

Conclusion

Cybersecurity and frameworks present opportunities for technical communicators willing to adapt and stretch their skill sets and to not be too focused on job titles. Cybersecurity is a well-paying career field that values and welcomes a varied skill set. Communication skills, technical skills, management skills, and software and systems skills at almost any level are highly used. Don't be afraid to speak up and apply for that job or express your interest in cybersecurity. Sharpen your technical skills and pursue a certification in something that interests you. Volunteer or offer to help on a project related to cybersecurity and frameworks. Many companies (including mine) offer "transition plans" for people looking to move into cybersecurity for other fields. Good luck!

DAWNELL CLAESSEN *(mail@dawnell.com) is a technical communicator and certified security systems professional (CISSP) specializing in security certification and accreditations of information systems operated by the Defense Health Agency and Veterans Health Administration. She works constantly with the NIST Risk Management Framework and the Cybersecurity Maturity Model. Dawnell holds a Master of Library and Information Science with a specialization in federal information policy from the University of Texas at Austin. For STC, Dawnell also acts as a co-manager of the Policies and Procedures Community and she is really hoping that this article will win her brownie points (and a polo shirt) with the Florida Chapter of STC's Active Member Program.*

REFERENCES

NIST RMF Framework. "New to Framework." Accessed 21 May 2021. *www.nist.gov/cyberframework/new-framework.*

Sayegh, Emil. "As the End of 2020 Approaches, the Cybersecurity Talent Drought gets Worse." *Forbes.* Accessed 21 May 2021. *www.forbes.com/sites/emilsayegh/2020/09/22/as-the-end-of-2020-approaches-the-cybersecurity-talent-drought-gets-worse/.*

The Missing Report. "Cybersecurity Frameworks 101 – The Complete Guide." Accessed 21 May 2021. *www.preyproject.com/blog/en/cybersecurity-frameworks-101/.*

Toolshero. "Communication Strategy Framework." Accessed 21 May 2021. *www.toolshero.com/communication-skills/communication-strategy-framework/.*

How to Cyber: A Cybersecurity Quick Start Guide

By JESSICA BEHLES

CYBERSECURITY IS A shared responsibility. Whether the CEO of a Fortune 500 company, an employee connecting remotely to the company network, a teacher using Zoom to conduct classes, or a parent simply trying to keep the kids safe, we must all do our part to make the Internet a safer place.

Indeed, cybersecurity should be a priority for anyone using internet-connected technology. For a technical communicator working with technology every day, both at work and in the home, a basic education in cybersecurity not only keeps you, your family, and your employer safe, but may also open up new opportunities.

When I stumbled into cybersecurity in 2013, I knew very little about the field despite being fairly technologically literate. I understood basic internet security, but I had much to learn before I could fulfill my duties. Furthermore, there is an overwhelming amount of information out there, and it is constantly changing. I muddled through, but I wish I'd had some guidance beyond the company's basic awareness training.

Because of these challenges, I created this "quick start guide" to help you hit the ground running with cybersecurity, whether you are an everyday user of technology or considering a career in the field.

This article is broken into beginner, intermediate, and advanced sections. Each section contains a list of resources you can use as a starting point for your education and research. "Beginner" contains the most basic information, similar to what a company might offer in its training and awareness program. "Intermediate" is for those who are comfortable with technology and wish to go beyond the basics to protect themselves against additional threats. "Advanced" is intended for those who are interested in pursuing a career in cybersecurity or simply want to know even more about the field.

Beginner

The resources and information in this section are similar to what a company with a robust security awareness program would provide to its employees. Because not all companies offer such programs, this information should not be neglected, even though it might be considered basic knowledge. Topics covered by the resources listed below include username and password hygiene, recognizing and avoiding social engineering, identity theft, malware, social media safety, and protecting some of the most vulnerable members of our society—such as children and seniors—online.

A good starting place to begin learning about cybersecurity is Stop. Think. Connect. (*https://stopthinkconnect.org/tips-advice/general-tips-and-advice*), which provides some simple, actionable tips to develop and practice good online safety habits. Check the Resources tab for tip sheets covering topics like passwords, safe online shopping, and ransomware.

A slightly more in-depth offering is the National Cyber Security Alliance's "How to Stay Safe Online" (*https://staysafeonline.org/stay-safe-online/*). This site provides information about keeping your information private, securing accounts and devices, and checking privacy settings on popular devices and websites. You can also learn what to do if you become the victim of a cybercrime.

The U.S. Federal Trade Commission's "On Guard Online" (*https://www.consumer.ftc.gov/features/feature-0038-onguardonline)* offers tips for keeping your personal information safe, such as using public Wi-Fi networks safely and recognizing social engineering. There are also resources for parents who want to learn to keep their children safe.

The SANS Institute—one of the largest cybersecurity research and training organizations—publishes *OUCH!*, a newsletter with a different security topic each month (*https://www.sans.org/security-awareness-training/ouch-newsletter*). Past topics have included passwords (April 2019), secure online shopping (November 2019), social media privacy (February 2020), and safe video conferencing (August 2020). Consider subscribing to ensure you don't miss future topics.

TERMS TO KNOW

Beginner

Data breach-The viewing, distribution, use, or modification of private data by an unauthorized party.
Cyberattack-A malicious attempt by an unauthorized party to view, steal, modify, or otherwise harm data or other resources.
Cyberbullying-The use of communication technologies to harass, threaten, intimidate, embarrass, or otherwise bully a person or people.
Malware-Malicious software created to steal information, disrupt processes, and otherwise cause harm. Examples include viruses, ransomware, spyware, adware, and rootkits.
Skimming - The theft of payment card data (e.g., credit/debit cards) using a mechanical device that impersonates a legitimate card reader. (Krebs, 2010)
Social engineering - Tricking or manipulating someone into taking an action (e.g., revealing information or sending money), often resulting in fraud. Phishing is a common form of social engineering.

If you are looking for more information about keeping your kids safe on the internet, CyberWise's Online Security Hub" (*https://www.cyberwise.org/online-security-hub*) is a resource site for busy grownups seeking to help youth use tech safely and wisely. This site has information and resources to help parents keep their children safe online at any age. It includes basic tips and guides and has aggregated hundreds of articles about youth online security from all over the internet.

Finally, for a mix of basic and more advanced information, you can visit the U.S. Cybersecurity and Infrastructure Agency's (CISA) internet "Tips" (*https://us-cert.cisa.gov/ncas/tips*). This site offers a broad assortment of information spanning from basic password advice and e-mail safety to home network security and encryption.

TERMS TO KNOW

Intermediate

Authentication: The process for confirming a person's identity before granting access to a computer system.
Authentication factor: A means of proving your identity. Three types: something you know (e.g., password or secret question/answer), something you have (e.g., hardware token or smart card), and something you are (e.g., fingerprint).
Encryption: The process of converting data into a form that is unreadable by humans, machines, or both. Decryption is the reverse process.
Internet of Things (IoT): Internet-connected devices, such as "smart" devices (e.g., phones, TVs, watches, thermostats, etc.).
Local Area Network (LAN): A network of systems connected via physical cables in a single location.
Multifactor authentication: The use of two or more authentication factors to verify your identity.
Patch: A software update provided by the software vendor, usually to fix errors and vulnerabilities or improve features.
Virtual Private Network (VPN): A digital connection between two systems or networks that is usually encrypted to protect data flowing between them. Often used by remote workers to access company resources.
Vulnerability: A bug or weak point in a system or software that can be exploited to gain unauthorized access or cause harm.

Intermediate

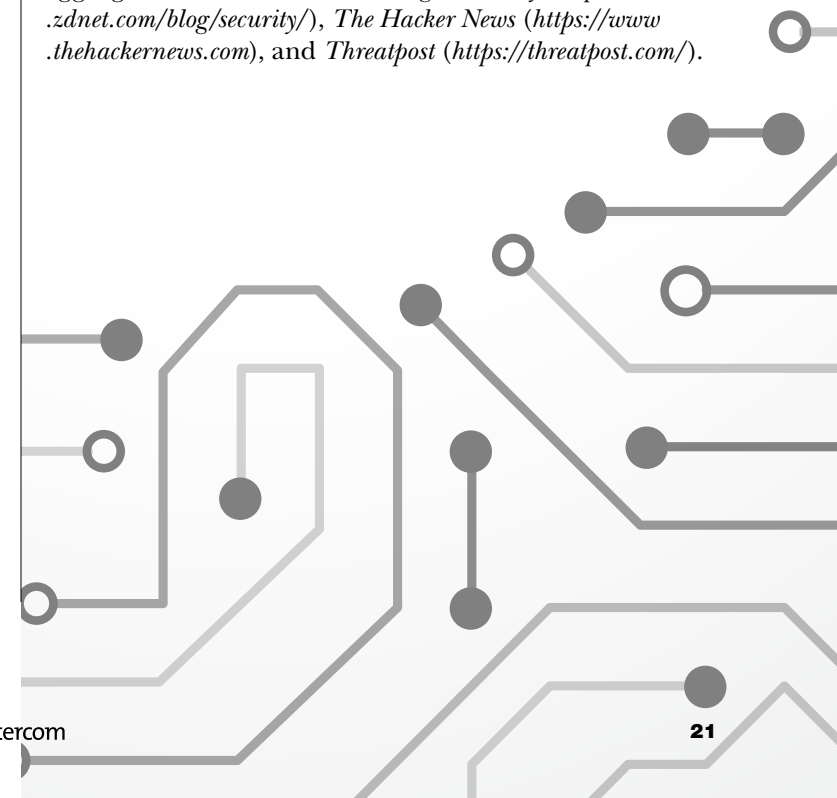
The information in this section is intended for those with a basic cybersecurity education who want to learn more about protecting themselves and others against additional threats. Topics covered by these resources include Virtual Private Networks (VPNs), mobile device security, Internet of Things (IoT) security, home network security, and encryption.

The FTC's Online Security portal (*https://www.consumer.ftc.gov/topics/online-security)* includes beginner topics like recognizing scams and reducing spam emails; however, you can also learn about more advanced means to protect yourself, like securing your home wireless network, using a Virtual Private Network (VPN), safely using mobile apps, and setting up Internet cameras (e.g., webcam, online surveillance camera, etc. securely.

I mentioned the CISA's Internet Tips website (*https://us-cert.cisa.gov/ncas/tips*) as a beginner resource, but it also covers topics like Denial Of Service (DoS) attacks, securing Internet of Things (IoT) devices, securing wireless networks, and threats like rootkits and botnets. Additionally, CISA offers a number of publications that cover many of these topics in greater detail.

Blogs can be a great way to learn more about cybersecurity. Two that are particularly well known and respected are Brian Krebs' *Krebs on Security* (*https://krebsonsecurity.com*)and Bruce Schneier's *Schneier on Security* (*https://www.schneier.com/*). While I personally prefer Krebs' investigative journalism over Schneier's style of aggregating and commenting on others' articles, both authors report on cybersecurity news and topics in an approachable manner that non-experts can understand and enjoy.

Other respected blogs and cybersecurity news aggregators include *Dark Reading*, *Zero Day* (*https://www.zdnet.com/blog/security/*), *The Hacker News* (*https://www.thehackernews.com*), and *Threatpost* (*https://threatpost.com/*).



TERMS TO KNOW

Advanced

Attack surface: The total number of vulnerabilities an attacker can use to break into an environment.

CIA triad (confidentiality, integrity, availability): The cornerstone of cybersecurity. *Confidentiality* means keeping data safe from unauthorized viewers or access. *Integrity* means ensuring that data are complete, accurate, and not tampered with in any way. *Availability* means ensuring that data or other resources can be accessed or used any time they are needed.

Defense-in-depth: Implementing multiple layers of redundant security measures to protect the CIA of data.

Ethical hacker: An individual who discovers vulnerabilities in systems and software and discloses them to companies for patching.

Firewall: Software or hardware that monitors data flowing through networks and blocks perceived threats.

Hardening: Configuring software or a system to reduce its attack surface.

Least privilege: Having access to only those resources that you need to perform your duties.

Security control: A safeguard or countermeasure in place to protect the CIA of a system or entity.

Advanced

If you find cybersecurity interesting, it might be worth considering for a career. It is a dynamic, growing field that is facing a well-documented shortage of qualified workers. Furthermore, many of the greatest challenges are due to individuals, rather than technology, and the solutions to these challenges often lie in skillful communication (Flores, 2018, Whatis.com. n.d.).

The resources in this category are intended for those who intend to pursue a career in cybersecurity or simply wish a more complete understanding of the field.

The SANS Reading Room (*https://www.sans.org/reading-room/categories*) is home to more than 3,000 white papers about various cybersecurity topics, with more being added each month.

Along with the blogs included in the Intermediate section above, *Infosecurity Magazine (https://www.infosecurity-magazine.com/)* and *SC Magazine* (*https://www.scmagazine.com/*) are great for expanding your knowledge and keeping abreast with news and changes within the field and threat landscape.

Anyone in cybersecurity should know about the *Verizon Data Breach Investigations Report* (*https://enterprise.verizon.com/resources/reports/dbir/*). Published each year by Verizon's Enterprise Services division, it aggregates and analyzes data about the previous year's data breaches to identify trends, new attack vectors, common tactics, attackers, victim profiles, and more. It is dense, but well formatted and readable, and I strongly recommend reading it every year.

If you prefer more guided training, the *awesome-infosec* GitHub (*https://github.com/onlurking/awesome-infosec*) has compiled an extensive list of training and college-level classes, many of which are free. Additionally, you can

Starting Topics

Cybersecurity is a large field, and it can be easy to get lost amid the sea of information. Here is a list of topics you might find interesting to get you started. It is by no means exhaustive; rather, it is meant to serve as a jumping-off point as you begin navigating this complex field.

- Assurance/audit
- Business continuity/disaster recovery
- Cloud security
- Cryptography
- Digital forensics
- Ethical hacking/penetration testing
- Firewalls
- Governance (policies & standards), compliance, oversight
- Identity and access management
- Information warfare
- Internet of Things
- Incident response
- Malware
- Mobile device security
- Network security
- Regulations (PCI DSS, GDPR, CCPA, HIPAA, etc.)
- Risk management
- Secure coding
- Social engineering
- Threat modeling
- Training and awareness
- Vulnerability management

search on Coursera for free or paid cybersecurity courses (*https://www.coursera.org/learn/security*). Finally, Cybrary (*https://www.cybrary.it/*) is a training platform geared for cybersecurity professionals. It has a monthly fee after a two-day free trial; however, it does offer some free courses, many of them changing monthly.

Another approach to diving into cybersecurity is to read the regulations and best practices that companies are often required to follow. It would be impractical to list all of them here, so here is a sample of the ones you are most likely to encounter:

The Center for Internet Security (CIS) (*https://www.cisecurity.org/controls/*) publishes a list of the top twenty best practices that allow organizations to efficiently reduce risk in their environments.

The General Data Protection Regulation (GDPR) (*https://gdpr-info.eu/*) is a law that dictates how companies must protect the personal information of European Union (EU) citizens. Any company doing business with EU citizens must comply or face fines in the millions of Euros.

HIPAA-The Health Insurance Portability and Accountability Act of 1996 (*https://www.hhs.gov/hipaa/index.html*) dictates how protected health information (PHI) must be collected, used, and safeguarded. All organizations handling PHI are subject to this law.

The National Institute for Standards and Technology (NIST) publishes a suite of more than 200 Special Publications (SPs) that focus on information security and cybersecurity topics and best practices. I recommend starting with NIST SP 800-53 (*https://csrc.nist.gov/publications/sp800*) and Security and Privacy Controls for Federal Information Systems and Organizations (*https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*).

NIST also produces a framework for improving critical infrastructure security. (*https://www.nist.gov/cyberframework*). Many organizations have adopted the Framework to guide their approaches to cybersecurity.

The Cybersecurity Maturity Model Certification (CMMC) is a program used to consistently measure cybersecurity implementation. This certification, which includes and expands on the controls in NIST SP 800-171, is required for U.S. Department of Defense contractors and subcontractors; however, many companies use this model to assess their own cybersecurity capabilities (*https://www.acq.osd.mil/cmmc/*).

Most financial companies are required to follow the Payment Card Industry Data Security Standard (PCI DSS) (*https://www.pcisecuritystandards.org/*), which focuses mainly on protecting credit card customers and other consumers of financial products.

JESSICA BEHLES *(j.e.behles@gmail.com) is currently a cybersecurity technical writer for Discover Financial Services. She has a BS in Technical Communication from New Mexico Tech and an MS in Technical and Professional Communication from UW-Stout. She also holds GIAC-GISF, GIAC-GSEC, and GIAC-GSTRT certifications and is studying for her CISSP. Jessica is enjoying the weather in New Mexico with her husband, two black Labs, and a black cat who rules the household.*

REFERENCES

Flores, Maria Antonieta. 2018.*The Language of Cybersecurity*. XML Press.

Krebs, Brian. 2010. "All About Skimmers." Krebs on Security. Accessed 21 May 2021. *https://krebsonsecurity.com/all-about-skimmers/.*

PCI Security Standards Council. n.d. "PCI-DSS Glossary." Accessed 21 May 2021. *https://www.pcisecuritystandards.org/pci_security/glossary.*

Whatis.com. "IT Career Management." Accessed 21 May 2021. *https://whatis.techtarget.com/.*

Developing Engaging Cybersecurity Training

By DR. LIZ HERMAN | *STC Associate Fellow*

PICTURE THE SCENE. You are looking at your computer screen. If you are lucky, the only sound is the soft click of the mouse button as you navigate because you muted the narration. As soon as the e-learning module allows, you move to the next page. You may be checking text messages on your phone while the e-learning page processes its content. You may switch to another screen on your computer and answer some emails, Google Chat with a colleague, or check out the STC Communities Slack workspace. Whatever you are doing, you are probably not paying full attention to the task at hand, which is completing your organization's annual cybersecurity training. How many of us sit through rote cybersecurity training clicking the "Next" button without ingesting or retaining any of the content? If the average cost of a cybersecurity attack, according to the Global Application and Network Security Report, costs $1.7 million, how can we ensure that organizational cybersecurity training is meaningful, and its content retained?

Technical communicators play two roles related to cybersecurity training. The first role is that technical communicators often serve as training developers employed in the development of cybersecurity training. Although not explicit to cybersecurity training, forty-five percent of technical communicators responding to Saul Carliner and Yuan Chen's Society of Technical Communication's 2018 Census noted that they had produced training and tutorial materials in the past 12 months. We can assume that some of that training was likely around the annual cybersecurity training that gets deployed. The second role is that technical communicators, along with other organizational employees and contractors, are recipients of said training. In either role, the question of how to make the training more engaging and meaningful may be top of mind.

Current State of Cybersecurity Training

To discover the current state of cybersecurity training, the author interviewed two experienced training managers and initiated a survey to collect additional perspectives. When asked about cybersecurity training, Doris Tempelmeyer, a strategic, goal-oriented training manager with an eye for process improvement, answered, "Compliance training. Two words guaranteed to get an eye roll. Compliance training needs a reboot." Cybersecurity training is often wrapped into what organizations call annual compliance training. Tempelmeyer listed the issues she sees with cybersecurity/compliance training: dry monologues, technical jargon, long and extraneous courses, and infrequency. Regarding the infrequency of the training, Tempelmeyer notes, "You don't consume a year's worth of vitamins in one meal, you take a daily dose." A survey respondent who self-identified as a trainer and cybersecurity specialist echoes Tempelmeyer's comments around infrequency. "I'm used to some pretty heavy-duty material. Training should be more frequent than once a year, it should be fully supported by management, and attendees should be tested on their comprehension and on their adherence to any key practices or policies."

Nancy Workman, Senture, LLC Training Manager, who works with the author, shared that she thinks about this topic often. She wonders, "How do we make it stick?" Workman laments the one-size-fits-all approach. In her environment, deploying the same cybersecurity training to a facilities manager and a contact center supervisor is not ideal because of the different roles and responsibilities. She states that trainees are "probably missing out on information we need or we're bored and tuning out to information we don't. While there will definitely be many topics that will apply to all, they each have unique situations and environments."

In a survey initiated in February 2021, the author collected responses by posting the survey URL on LinkedIn and Twitter. Forty-one individuals responded to the 12-question survey that asked about their engagement in cybersecurity training, their training design preferences, and their thoughts around how to improve this type of training. Results point to a needed overhaul:

- 39% rated their engagement during cybersecurity training as moderately to highly disengaged;
- 56% did not think that cybersecurity training helped them prevent cybersecurity attacks within their organization;
- 71% marked true that they navigate through cybersecurity training as fast as it allows them to finish; and
- 76% marked true that they find cybersecurity training to be largely repetitive and boring.

Regarding what design elements are preferred, respondents were less enthusiastic about text-based, narration-based, and gamified (e.g., treasure hunt activities) training modules. However, respondents also said they wanted more audio, video, and gamification. It may be beneficial for training developers to understand what works best for their specific organizational audience.

The open-ended questions asking about improvement yielded rich results for training developers. When asked how cybersecurity could be improved, respondents commented on frequency, duration, real-world examples, and training variety and design:

- "Offer it more frequently. We're all potential victims!"
- "Send us training more often! We need it."
- "It might be better to be spread out over several days. Like a daily tip for a week or similar. Grinding an hour or two at once is brutal."

- "Try and rotate different delivery methods (e.g., one year it is online, the next year it is a group meeting, next year it is a workshop, etc.)."
- "More real-world examples of breaches and how they were done and the consequences."
- "Real examples and consequences such as news stories or direct company impacts. Don't try to be cute."
- "My company gives the exact same training every year. Mixing things up could make it more interesting and engaging."
- "Emphasize new best practices, deemphasize stuff we've already known for years (like don't write down your passwords)."
- "Tell me what has changed since last year; give me things in action (action-based learning)."
- "Don't make me click on 10 different boxes on one slide to get the info."
- "Tell us something we don't know. We've all had data breaches. Talk about risks of using the web while on work machines."

When offered the chance to tell the training department how to improve cybersecurity training, survey respondents requested cheat sheets, reminders of key lessons learned, and to stop deploying the same material every year. One respondent noted how the current pandemic should reshape cybersecurity training. "Show how it impacts people at home as well as work. That way they can have good habits that carry back." Another suggested that the training department slow users down by making them answer a question before moving on to new content to avoid the "clickety clack, don't look back" approach to taking cybersecurity training, which is to get it over with and finish it as soon as possible. Another pleads to use specific company examples that will resonate with the trainees. "Use actual company examples instead of buying canned training that refers to 'your company' on every slide."

Because cybersecurity training is sometimes developed or selected and deployed by the information technology (IT) department and not the training department, the survey included a question asking respondents what they would say specifically to IT about improving cybersecurity training. Survey respondents asked for an understanding of and focus around the biggest, specific risks that trainees may face. They also asked for role-specific training. "Different departments have different vulnerabilities. If I'm 100 percent onsite, I have different risks than the salesperson who's on dodgy public Wi-Fi and using random flash drives." One respondent asked for the internal cybersecurity team to deliver the training rather than using "monotonous and canned training videos." They asked for IT to help them help themselves when it comes to cybersecurity. "Help me by integrating security features with the tools I use. For example, my IT department has updated our Microsoft Office tools to make it easy to add appropriate classification to every document." Another simply stated, "Make sure the button to flag spam is in every version of Outlook installed for folks."

Two respondents mentioned accessibility and diversity and inclusion. "Make it American Disability Act (ADA)-compliant by making sure graphics don't cause seizures." "Space out the quiz checks, provide a transcript or closed captioning, have speakers that are clearly understood, and videos that are culturally appropriate."

Improving Cybersecurity Training

Survey results indicate a desire for better, more engaging cybersecurity training. What can training developers do to improve training? Tempelmeyer says, "People

learn when they are motivated, not when mandated. To gain better interest, remove the task of Compliance Training from the legal advisers, IT team, and safety committee. Think like a marketing team. Customers buy experiences, not products." Workman says, "Use scenario-based interactive activities. Make it personal to me. Challenge me to begin thinking about ways it [cybersecurity breaches] could happen to me. Finally, clearly communicate and stress the consequences. If I know and understand the devastating results on me, my team, our client, and my organization of failing to use security best practices and policies I am going to be more cautious." Regarding making it personal, Tempelmeyer adds, "Frame the lessons with the employee as the hero in the story, not the victim. Make them the protector."

Tempelmeyer provided specific actions to take to counter some of the most common issues:

- **Dry monologue presentations**. Impactful training needs to engage the learner's mind. Long winded monologues, reading every slide verbatim is death by PowerPoint. Talk with the class, not at them. The delivery method is what causes people to learn. For improved engagement, implement High Impact, On Demand (HI-OD) assets such as audio/video, simulations, and conversations. Game simulation exercises are another great way to stimulate the production of endorphins in the learning process.
- **Technical jargon.** Technical talks are not conducive to the learning process. Effective communication is about the recipient, not the speaker. Know your audience and speak in terms that they understand. Use stories and analogies that are meaningful to the learner. Consider Federal Plain Language Guidelines.
- **Infrequent**. If you don't use it, you lose it. Annual training is not habit forming. One of the best habits a learner can instill is self-quizzing to recalibrate their understanding. The forgetting curve hypothesizes the decline of memory retention in time. Retrieval Practice Activities (RPA) are routine exercises that aid in the retention of knowledge. Practice that is spaced out, interleaved with other learning, and varied produces better mastery, longer retention, and more versatility. The spacing of practice allows for forgetting, which requires effort to retrieve. The cycle of forgetting and reconsolidating knowledge further strengthens memory. In practice, this may look like a daily quiz question when you log into the system.
- **Long, extraneous courses.** Too much data pitched without pause. Lesson segmentation is needed. Microlearning involves short, focused learning (three to five minutes) designed to meet a specific learning outcome through routine, informal training. Again, a morning exercise is a great example.
- **Accountability.** If meaningful is the carrot, accountability is the stick. With most programs there is little accountability with failed compliance. What would happen if when you failed your morning quiz, you were locked out of the system and required to ask your supervisor for access to a retraining course? The positive reward side may involve public recognition of all teammates or departments who received perfect marks for the week.

According to Tempelmeyer, the bottom line with cybersecurity training is to sell it through meaningful, personal storylines; engage trainers via interactive learning and dialogue to communicate on their level; use segmented, microlearning lessons; and track learning with routine RPAs.

Summary

Is all cybersecurity training in need of improvement? No. Survey respondents mentioned that cybersecurity training did improve their awareness. "We are given periodic 'tests' where we get emails that are supposed to look like phishing emails to see how many employees will click a bad link. I feel like this has made me very aware of what to look for in emails that come through that I am not certain about." Another respondent who self-identified as a member of the U.S. Military mentioned Ray Semko as delivering the best in-person training on the subject that they had ever received. For cybersecurity training that can benefit from an overhaul, this article provides some perspective and a place to begin.

DR. LIZ HERMAN (*liz@lizherman.com*) *is an STC Associate Fellow and a member of the STC Nominating Committee. She writes, speaks, and teaches on technical communication, project management, and knowledge management topics.*

REFERENCES

Carliner, Saul and Chen, Yuan. 2018. "Who Technical Communicators Are: A Summary of Demographics, Backgrounds, and Employment." *Intercom* 65, no. 8: 8-12. *https://www.stc.org/intercom/2019/01/who-technical-communicators-are-a-summary-of-demographics-backgrounds-and-employment/.*

Radware. 2020. Protecting What You Can't See: Global Application & Network Security Report: Eliminating Security Blind Spots in an Age of Technological Change." Accessed 21 May 2021. *https://www.radware.com/ert-report-2020/.*

Semko, Ray. n.d. "Ray Semko: The Dice Man." Accessed 21 May 2021. *https://raysemko.com/.*

Society for Technical Communication. n.d. "STC Communities Slack Workspace." Accessed 21 May 2021. *https://www.stc.org/membership/slack/.*

Beyond the Weakest Link: Maturing End User Information Security Education to Bolster Organizational Defenses

By VALERIE VOGEL and JOANNA GRAMA

WE OFTEN THINK of information security as a technology discipline with technological solutions implemented by technical experts. This first line of technical defense is backed up by policies and processes telling end users what should, or more often shouldn't, be done to help protect the organization. Logically, this makes sense because cybersecurity is generally broken down into three essential components: people, processes, and technology. However, an organization's information security program is not just about firewalls, phishing users, and acceptable use policies. Over the past several years there has been a shift in how we approach information security more strategically by focusing on the people and human risks.

Farewell FUD and the Weakest Link

This change has been a long time in the making. Information security is fundamentally about stopping bad things from happening or reducing their impact when those bad things do happen. As a result, information security professionals have often been accused of relying on fear, uncertainty, and doubt (FUD) to implement information security controls and safeguards and to advance the missions of information security. Using FUD to make a business case for information security relies on a psychological response, even in an organization, to avoid the fear-triggering event. It's a pessimistic tactic that is more likely to be denounced as the profession continues to mature.

The profession has also used a similarly pejorative tactic when referring to end-users as the weakest links in protecting an organization's information security posture. The term refers to a person in a situation who is less knowledgeable or skillful than others. Information security professionals would identify end-users as the weakest link to support implementing technical controls and safeguards to manage end-user behavior, rather than taking a constructive approach to educating users and helping them improve their understanding of information security risks and best practices.

The 2020–2021 global coronavirus pandemic has propelled information security educators, training personnel, and communicators to drastically reconsider how we educate users about information security practices. The quick move to remote work has heightened the need to make sure that users are informed about and empowered to implement information security practices in their remote working environments because technical controls can't always work in an environment not managed by a central IT organization.

It hasn't been easy. Everyday challenges exacerbated by the pandemic include:

- **Users are overloaded with information.** We live in a society where 24/7 news channels label every story as "breaking news," and email, chat, and social media feeds are full of "information you need to know today!" The glut of communication, most of which is digitally delivered and not personally conveyed, makes it easy to ignore the deluge or to tune out communications that seem repetitive. With multitasking as the norm, attention is fleeting.
- **Users are feeling burnt out.** The early days of quarantine enthusiasm and pandemic bread baking are over. We have settled into a new routine of quarantine monotony and many people are mentally exhausted or fatigued from ongoing stay-at-home orders and the attendant responsibilities. Anyone facing personal challenges at home may not view work-related priorities with the same sense of urgency or importance amid a pandemic.
- **Users are working from everywhere and logging more hours online.** People are working from everywhere with a combination of business-owned and personal devices. This mix makes it more challenging for organizations and information security practitioners to secure and protect organizational devices, and more importantly, data. In addition, recent research shows the remote workday is lengthening, meaning that organizations need to be mindful of the need for around-the-clock monitoring and review to keep information and systems safe.

So how can we break through the noise and get creative in educating an audience that is key to protecting organizational data, information systems, and devices? Across industries, we are seeing new gamified awareness and education approaches to engage and motivate users, including virtual escape rooms, digital scavenger hunts, online games and puzzles, public service announcements (PSAs), six-word projects, and even haikus. These meaningful and *fun* educational approaches can be cultivated to encourage and empower people to reach out for assistance when confronted with a new information security threat. No longer the weakest link, users are now the first and last lines of defense and a critical part of the early warning system for organizational information security programs. As the National Institute of Standards and Technology (NIST), the National Cyber Security Alliance (NCSA), and countless other organizations have stated, "Cybersecurity is everyone's job."

Thinking Strategically About Information Security Education

Incorporating information security awareness and training into a broader information security program is nothing new. Awareness and training activities are recognized as a key component of most information security best practices frameworks. For instance, the Awareness and Training Control Family in the popular NIST information security framework requires the

development of an awareness and training policy and responsible authority. It also requires training activities on specific topics such as insider threat, as well as additional training based on a user's role in an organization. The control family also outlines requirements for maintaining training records and gathering feedback. Unfortunately, the control family does not outline how to provide this training as a strategic component of an organization's information security program, nor does it outline how to provide effective and successful training.

Thinking strategically about technical communication is not new, but it is something that the information security profession has struggled with, likely because of the lack of technical communicators in the information security profession. For instance, recent reports from the SANS Institute, a prominent source for information security research, suggest that almost 80 percent of information security awareness professionals come from a technical background, while less than 20 percent have a non-technical background like communications and marketing professionals. While technical experts will have a strong grasp of the information security subject matter, they may not be as well-versed in training methodologies or the best ways to construct educational messaging. Strategic planning brings those perspectives together to create a comprehensive approach to information security education.

Most strategic planning processes are organized as a cycle that helps an organization understand where it's been and where it wants to go. This type of planning can easily be applied to information security educational activities.

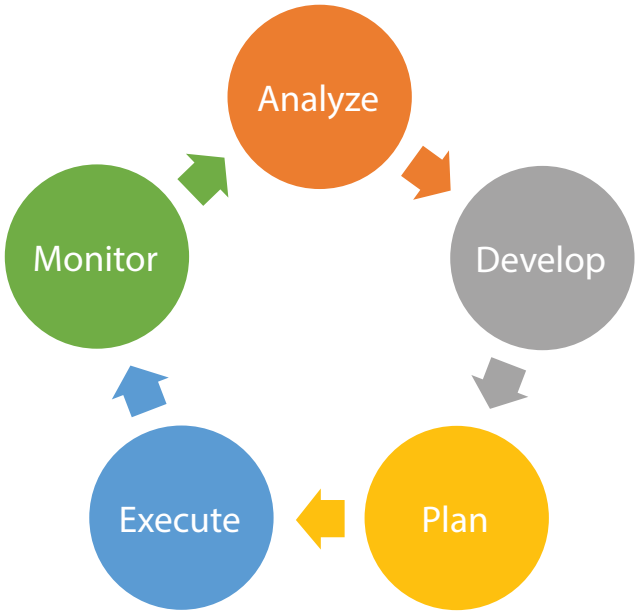


Figure 1. Strategic planning processes organized as a cycle

During the **analyze** stage, an organization reviews its business strategy, historical performance, and the threats that it faces to understand its current context. From an information security education perspective, the organization will review past awareness and training activities, the perspectives of its audiences, and the threats to a successful awareness program.

Following this analysis, the organization will **develop** a mission and vision for its information security education program. During this phase, the organization outlines the goals for the education program at both an organizational and stakeholder level. When considering stakeholder needs, the organization should consider the needs of different organizational audiences (e.g., leadership, management, individual contributors) and how information security messaging must be tailored to the role of each group.

During the **plan** stage, the organization conducts a gap analysis to understand how it will move from the current educational state to the future planned state. Often the gap analysis activity leads to the creation of a roadmap, which helps to outline what the organization wants to achieve and how it will accomplish the proposed goals during certain timeframes.

The **execute** stage is where the previous review and planning activities pay off. During this stage, the organization starts the work of executing its roadmap. From organizing events to creating awareness materials, this stage is characterized by project plans, budgets, and leading and coordinating the work of multidisciplinary teams.

No higher-level strategic planning process is complete without a phase that **monitor**s performance and progress. As projects are completed and the organization moves forward on its information security education roadmap, measuring performance and ensuring alignment with the previously outlined mission and vision are crucial. As strategic planning is a process, not a project, the results from the monitor phase feed into the analyze stage for cyclic revisions to the plan.

Measuring the Impact of an Information Security Awareness Program

Assessing and measuring the impact of an organization's security awareness and training program can provide insights into the effectiveness of the educational activities offered to end-users. Relevant metrics can help illustrate how program goals are being met and offer concrete data that can be shared with senior leadership.

Some sample metrics frequently used to measure security awareness program activities include the following. Note that many of these are compliance-based and may not demonstrate the true impact or reach of a more mature program:

- How many people participated in the security awareness workshop, presentation, online quiz, virtual escape room?
- How many people completed the mandatory (annual) online security awareness training module?
- What is the percentage of students, faculty, and/or staff who have received information security training (measured over time)? Has there also been a reduction of information security incidents (also measured over time)?
- For organizations running phishing campaigns via email or SMS, what were the open rates (i.e., how many recipients opened the test email/text), click rates (i.e., how many recipients clicked on the phishing link or downloaded an attachment in the test email/text), and report rates (i.e., how many recipients reported the test email/text to the help desk or IT team)?

Broader organizational metrics for an information security awareness program might include:

- What is the percentage of organizational IT budget spent on the information security awareness, training, and education program (measured over time)?
- How many people are managing the organization's security awareness and education program (total number of FTEs)?
- What is the percentage of organizational IT staff who receive additional training on how to incorporate information security best practices into their daily job function (measured over time)?

Besides the metrics mentioned above, consider including some "outside the box" key performance indicators (KPIs). While these suggested KPIs might not provide measurable values for an organization, they can be used to demonstrate some of the important work being done through an information security program to raise awareness and build community.

- Are people reaching out to the infosec team, IT staff, or the help desk with questions about security? A good security awareness and training program should create and encourage opportunities for dialogue with users across the organization. Consider tracking the number of emails, phone calls, or Slack messages from employees about security-related issues, which may signal that users trust the infosec or IT team and see value in the team's expertise.
- Are partnerships being built across the organization with other departments like marketing, finance, or operations? Developing and nurturing relationships can help people understand and appreciate the role of a security awareness professional and why training is so important.
- Are security ambassador programs being leveraged to help boost information security awareness efforts across departments? For organizations that do not have a dedicated security awareness professional, an IT team can identify volunteers to help share security awareness communications and educational resources. Track the number of ambassadors (also referred to as champions or advocates), the number of employees each ambassador reaches, and the number of communications shared by the ambassadors.

Seizing Opportunities to Change Security Awareness and Education

Winston Churchill stated, "A pessimist sees the difficulty in every opportunity; an optimist sees the opportunity in every difficulty." Security awareness professionals and technical communication professionals who are tasked with information security educational roles are constantly finding new opportunities to take an optimistic approach. Rather than allowing current

challenges like limited attention spans to become obstacles, we've observed people trying more creative approaches to develop useful (and witty) content to reach diverse audiences. We weren't expecting sea shanties to become popular in the 21st century, but why not embrace this entertaining trend? There is already one security-themed sea shanty written by a well-known social engineer and hacker, Rachel Tobac, which might provide inspiration.

Sea shanties are just one example of modern, engaging content that can be leveraged for end-user awareness. Another approach for our growing work-from-anywhere culture might be to host regular virtual office hours or "Ask Me Anything" (AMA) sessions. Offering informal chances for users to bring their security questions or concerns to an expert can demonstrate how approachable the team truly is and might offer a welcome break (and some levity) in people's workday. These slightly unconventional approaches to education can encourage curiosity and create opportunities for ongoing dialogue between educators and users. The content is fun, doesn't present information in an overwhelming way, and shouldn't cause people to overthink security or feel intimidated. Other creative examples can be found on social media, in publications, and online forums, or simply by talking with our peers. If we want to continue seizing these moments to proactively educate people about cybersecurity in more organic and meaningful ways, we should continue sharing ideas within the community.

People, processes, and technology will continue to be the primary pillars of cybersecurity. But perhaps by intentionally shifting our focus to people, empathy, and authentic engagement, we can help make information security more inclusive and accessible to users.

JOANNA GRAMA (*joanna.grama@vantagetcg.com*) *is an Associate Vice President at Vantage Technology Consulting Group. She has more than 20 years of professional expertise in law, higher education, information security and risk, and data privacy. Joanna's passion is helping organizations successfully evolve their information security, privacy and risk programs.*

VALERIE VOGEL (*Valerie.Vogel@VantageTCG.com is a Strategic Consultant at Vantage Technology Consulting Group. She has more than 20 years of experience in higher education information security, focusing on program management, awareness and education program development, and community building activities. Before joining Vantage, she was Senior Manager of the EDUCAUSE Cybersecurity Program.*

REFERENCES

Learn more about information security awareness professionals and information security education programs with these resources.

Barker, Jessica. 2019. "The Human Nature of Cybersecurity." EDUCAUSE Review. Accessed 25 February 2021. *https://er.educause.edu/articles/2019/5/the-human-nature-of-cybersecurity.*

EDUCAUSE podcast. 2020. "Privacy and Security: The Six Words Project." Accessed 25 February 2021. *https://er.educause.edu/blogs/2020/9/privacy-and-security-the-six-words-project.*

Grama, Joanna. 2017. "Metrics Mania! Review." EDUCAUSE Review. Accessed 25 February 2021. *https://er.educause.edu/blogs/2017/9/metrics-mania-review.*

Harvard University. 2021. "Cybersecurity Awareness Month Digital Scavenger Hunt." Accessed 25 February 2021. *https://security.harvard.edu/ncsam-2020-digital-scavenger-hunt.*

Mancini, Steve. 2019. "Cyber Security Training Haikus: No Heads in the Sand." BlackBerry ThreatVector Blog. Accessed 25 February 2021. *https://blogs.blackberry.com/en/2019/05/cyber-security-training-haikus-no-heads-in-the-sand.*

Renner, Rebecca. 2021. "Everyone's Singing Sea Shanties (or Are They Whaling Songs?)." *The New York Times.* Accessed 25 February 2021. *https://www.nytimes.com/2021/01/13/style/sea-shanty-tiktok-wellerman.html .*

SANS. 2019. "2019 SANS Security Awareness Report." Accessed 25 February 2021. *https://www.sans.org/security-awareness-training/reports/2019-security-awareness-report.*

Spitzner, Lance. n.d. "Security Awareness Metrics." Accessed 25 February 2021. *https://www.sans.org/security-awareness-training/blog/security-awareness-metrics.*

Temple University. 2020."Student Cybersecurity Awareness Month Public Service Announcements." Accessed 25 February 2021. *https://sites.temple.edu/care/multidisciplinary-learning/mel-activities/.*

Tobac, Rachel. 2021. Sea shanty post. Twitter. Accessed 25 February 2021. *https://twitter.com/racheltobac/status/1352409636792492035.*

University of Virginia. 2020. "Virtual Escape Room." Accessed 25 February 2021. *https://security.virginia.edu/Cybersecurity-Awareness.*

Woelk, Ben. 2019. "Wind, Trees, and Security Awareness." EDUCAUSE Review. Accessed 25 February 2021. *https://er.educause.edu/blogs/2019/9/wind-trees-and-security-awareness.*

Compliance for Technical

Careers Communicators

By KAT REIERSON

Have You Considered a Career in Compliance?

Do you enjoy documenting processes? Do you thrive when asked to research rules and regulations? Then you might like a career in compliance writing. Detailed-oriented compliance writers leverage the knowledge of industry regulations and standards to create documents such as Standard Operating Procedures (SOPs).

According to Gan Integrity, effective corporate compliance is the ability to lead large groups of people toward achieving certain standards of conduct. Every business has to comply with rules, regulations, directives, and codes. Here are a few regulations, standards, and legislation with which organizations may need to comply:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Federal Information Security Management Act (FISMA)
- California Consumer Privacy Act (CCPA)
- General Data Protection Regulation (GDPR)

You are probably familiar with government regulatory agencies such as the Federal Trade Commission (FTC) and the Food and Drug Administration (FDA), but did you know that there are also numerous industry-specific associations and groups? For healthcare, there is the Office of the National Coordinator for Health IT (ONC), the Centers for Medicare and Medicaid Services (CMS), and many other compliance requirements. Corporate compliance covers both internal policies and procedures, as well as federal and state laws. In the cybersecurity industry, "compliance" means meeting various controls (usually enacted by a regulatory authority, law, or industry group) to protect confidentiality, integrity, and data availability.

Many organizations today have created entire compliance departments to manage compliance risks and ensure they pass compliance audits. Detection of non-compliant practices may result in heavy penalties and hurt their brand. The ever-increasing complexity of regulations has become an increasingly common business concern. Career opportunities in compliance exist with private industrial organizations, regulatory bodies, and nonprofit organizations across many industries, including healthcare, information technology (IT), and cybersecurity.

According to Mary-James Young, Senior Compliance and Regulatory Counsel, the field of compliance has been transitioning from being made up of a small group that "know what we mean" to a larger audience that includes outside auditors who "know what the document says… not what was meant." Because of the reliance of non-subject matter experts on written compliance requirements, clear, concise writing is more important than ever, and companies are starting to realize this. Clear, understandable documents enhance credibility and improve auditors' perceptions, which is where technical communicators come in (Young, Mary-James, 2014).

Technical communicators have the technical skills of subject matter experts (SMEs) and many of the skills required of compliance professionals: Expert verbal communications and conflict management skills, paired with patience, persistence, and an understanding of compliance standards and requirements. You have likely either worked on, or encountered, a compliance document during your career. Many of the companies we work for have to meet compliance requirements from various organizations such as the International Organization for Standardization (ISO), Underwriter Laboratories (UL), the Food and Drug Administration (FDA), among many others. Perhaps you have reviewed an SOP (Standard Operating Procedure) for clarity. If you enjoy documenting processes and procedures to meet various international standards, or understand the nuances and factors that impact policies, compliance writing might be a great career option for you.

Technical communicators work to contextualize complex information in ways that enable readers to perform needed actions. Most compliance frameworks provide requirements needed to reach the desired state, but they are not normally specific in how those requirements are implemented. The ability to understand how to make compliance frameworks actionable depends on an understanding of both the requirements and the organization's culture, with an

Acronyms

CCPA: California Consumer Privacy Act
CMS: Centers for Medicare and Medicaid Services
FDA: Food and Drug Administration
FISMA: Federal Information Security Management Act of 2002
FTC: Federal Trade Commissions
GDPR: General Data Protection Regulation
HIPAA: Health Insurance Portability and Accountability Act of 1996
ISO: International Organization for Standardization
ONC: Office of the National Coordinator for Health
PCI-DSS: Payment Card Industry Data Security Standard
PA-DSS: Payment Application Data Security Standard
SSAE: Statement on Standards for Attestation Engagements
SME: Subject Matter Expert
SOC: Service Organization Control
SOP: Standard Operating Procedure
UL: Underwriter Laboratories

emphasis on ensuring that various audiences clearly understand their obligation.

Here are some typical job titles from technical communicators interested in working in compliance:

IT Compliance Specialist/Technical Writer

- Write and/or edit technical documents, including policies, procedures, and work instructions. Develop outlines and drafts for review and approval by technical engineers, developers, and compliance management, ensuring that final documents meet applicable technical industry and compliance standards.
- Provide expertise in creating, implementing, and maintaining appropriate policies and procedures to comply with applicable technology, regulatory, and compliance requirements, including PCI-DSS, PA-DSS, SSAE 18 (SOC 1 Type II) SOC 2, GDPR, and HIPAA.
- Consult relevant regulatory, information sources and resources, and technical documents to obtain background information, and verify that pertinent guidelines and regulations governing technical documentation deliverables are applied.

Quality Associate /Technical Writer

- Liaise with operations personnel and application developers/business analysts to understand product details and operational workflows.
- Document the operational user stories and standard operating procedures for system enhancements and new products. This documentation is expected to be high quality and appropriate for use by operations personnel (customer support and laboratory operations).
- Author test scripts for all business processes and systems. Ensure these test scripts are updated when systems or products are changed.
- Contribute to the continuous improvement process outlined in the business quality manual.

Compliance Technical Writer

- Develop detailed examples of audit-ready documentation packages for reference architectures that meet the requirements of the FISMA, PCI-DSS, and HITRUST compliance frameworks for the Tanzu Kubernetes Grid line of products. An example of the type of documentation you will produce can be seen at *https://docs.pivotal.io/nist/index.html* and *https://www.fedramp.gov/templates/*.
- Update and improve the security control documentation as the reference architecture evolves, new products are added, and new compliance frameworks are added to the scope.

If you are interested, many professional organizations offer seminars and workshops around technical and regulatory writing. One of the best things about compliance is that nearly every industry has some compliance aspects and needs.

KAT REIERSON *(kell1017@umn.edu) is a technical writer at DocuSign passionate about crafting user-friendly content. She received her M.S. in scientific and technical writing from the University of Minnesota and loves naps, kayaking, and binging documentaries with her Bernese mountain dog.*

Learning Resources

Center for Professional Advancement - Writing for Compliance Course
https://www.cfpa.com/CourseDescription/CourseDescription/0/2916

Compliance Online - Technical and Regulatory Writing for FDA Regulated Industries Course
https://www.complianceonline.com/technical-regulatory-report-writing-for-e-submission-sops-protocols-clinical-trial-and-marketing-approval-applications-seminar-training-80237SEM-prdsm

REFERENCES

Pluta, Paul L. 2019. "Technical Writing for Compliance Part 1." Institute of Validation Technology. Accessed 11 May 2021. *https://www.ivtnetwork.com/article/technical-writing-compliance-part-1-overview.*

Daxko. n.d. "IT Compliance Specialist / Technical Writer" (Job Description). Accessed 21 May 2021. *https://jobs.smartrecruiters.com/Daxko1/743999684971418-it-compliance-specialist-technical-writer.*

Lensa. n.d. "Quality Associate / Technical Writer Job (Job Description). Accessed 21 May 2021. *https://lensa.com/quality-associate--technical-writer-jobs/kalamazoo/jd/9d4c76fdc4b7a6a0a5a542a6ddcffcf6.*

Lensa. n.d. "Compliance Technical Writer - Opportunity for Working Remotely Job" (Job Description). Accessed 21 May 2021. *https://lensa.com/compliance-technical-writer-opportunity-for-working-remotely-jobs/washington/jd/93c730461b732c5025f8442608043a58.*

Kelly, Matt. 2019. "What is Corporate Compliance and How Does It Impact Business?" GAN Integrity. Accessed 21 May 2021. *https://www.ganintegrity.com/blog/what-is-corporate-compliance/.*

Young, Mary-James (Jami). 2014. "Powerful, Persuasive Writing for Compliance Success." Vectren Corporation. Accessed 21 May 2021. *https://assets.corporatecompliance.org/Portals/1/PDF/Resources/past_handouts/Utilities-Energy-Compliance-Ethics/2014/P3PowerfulPersuasiveWritingforComplianceSuccess_3.pdf.*

CYBERSECURITY & DOCUMENTATION:

Security Considerations for Authors

By BRIDGET KHURSHEED

SECURITY IS A concern for technical communicators now more than ever. Cyberattackers thrive on opportunity. For example, rogue actors were exploiting COVID-19 as soon as the pandemic started. This article examines the risks and the solutions, or at least mitigations, that technical communicators can put in place now, along with best practices for yourself and your team. I first gave this article as a TCUK 2018 presentation, but while time has passed, and specific malware has evolved and changed names, the message remains the same.

Security: The More It Changes, the More It Stays the Same

One big change is that we now know our data is valuable. It is used by everyone from social media platforms advertising to data gathering organizations voter profiling during Brexit and recent U.K. and U.S. elections. This value is exploitable because more of our lives are online. For example, in my industry (financial technology, known as "fintech"), former ING CEO Ralph Hamer said in 2017, "We want to be a tech company with a banking license." But while current circumstances conspire to make it easier than ever to gather our data even for apparently innocent activities like targeted advertising and market research, companies may not always be aware that they are under the same level of scrutiny by bad actors.

Long-term reconnaissance using open-source intelligence (OSINT) and less legal methods, is a part of all attack preparations. And, unfortunately, there is no guaranteed protection whether your organization is tiny, has a "less interesting product," or is a low-key charity: you may still be the entry-level practice for an apprentice hacker or a key trust component gathered for a spear phishing attack. High schools have been hacked to get access to senior executives whose children attend the schools. In the U.K., the Woodland Trust charity had its shop and systems knocked out by ransomware this past holiday season. Information security is, therefore, everyone's business if we are going to make it work, and not just IT's and the cybersecurity team's concern. Consider this: it looks like the definition of information that needs to be kept safe is a little fuzzier than we might previously have thought.

So how does this affect technical communicators?

Why Your APIs and Docs Are Already a Target

The question to ask first is, what are the goals of the attackers? Money and data come first, then we could add "celebrity" in the hacker community, and even training. As we have mentioned, no company is too small to escape notice. It isn't just software companies like health, government offices, and many more that suffer the attention of bad actors. But at the top end

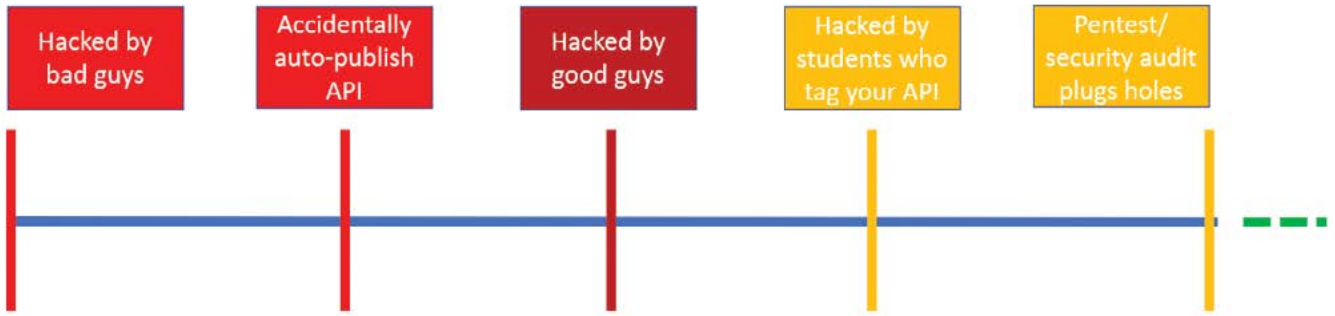

Hacked by bad guys
Accidentally auto-publish API
Hacked by good guys
Hacked by students who tag your API
Pentest/ security audit plugs holes

Figure 1. The vulnerability spectrum: A slightly tongue-in-cheek threat spectrum

of global information reconnaissance, the global API attack landscape is lucrative, mature, and well-defined. The Payment Services Directive (PSD2) means that banks operating in the E.U. must now have open APIs with potentially rich pickings. But even before that, operations security (OPSec) experts like Stuart Peck at ZERODAYLABS were saying, "APIs are the first place we look." For security experts, the API—and by extension all company documentation—is useful when preparing for an attack. OSINT is data collected from publicly available sources to be used in an intelligence context; That is, what can be viewed more or less legally.

Online documentation is so interesting because of the gems it may contain, everything from names of colleagues, email address structure, what programming language is used, implementation details, and even hardcoded passwords! If it is auto-generated and not checked, it may be that the bad actors are the first to see this. API issues blur the line between code and docs and so become the communicator's problem, too. An example can be found in a 2019 OWASP talk given by Skip Hovsmith, Principal Engineer and VP Americas Critical Blue. He, like Stuart Peck, describes "new business opportunities" appearing as a result of public APIs. He points out that APIs are well documented at a time when reverse engineering has never been easier and sums up some danger areas:

- Structured styles like REST are often easy to guess
- Leaky APIs may disclose implementation details and error handling
- Hidden APIs may be accidentally exposed by autodoc services

We will talk about those a bit more later.

Security: What Are the Risks?

Before we get more specific, let's take a look at what the results of this material being available to bad actors might be. We agree docs are targets, but what is the worst that can happen? Maybe we can live with it?

We hope that we catch doc issues in our review cycles over at the green end of the spectrum (that is omitted in Figure 1). We also hope after that that it's the good actors who attack us either as part of an official pentest/security audit or bounty hunters who will let us know the problem privately so we can fix it. If it is a bad case, it costs money, prestige; sometimes all access to systems is blocked and sometimes companies never get back on their feet. This assessment of risk is what your information security team should be deciding, but don't you want to be part of the conversation when you are the one writing the docs?

> Any organization in any field may be revealing more than they know.

Targets and Attacks

If attacks need targets, what are they? If you are a technical communicator working in software, it is clear that offering help in hacking your product is a bad idea. But any organization in any field may be revealing more than they know, and it is a constant review process. The first step is checking your APIs for elements that give the game away. Auto-generation tools can pull in code details, company information such as names and emails—not to mention evidence of a lack of professionalism, such as documented examples online of bad language in code naming slipping through! Your

APIs are objects of close scrutiny using easily available specific tools to trawl through; for example, GitHub repositories locating email forms and passwords, etc., such as truffleHog and gitrob. Other more technical vulnerabilities include:

- Certificates–training users to click popups or accept the fact that a certificate isn't right
- Loosely defined or leaky data–see my Twitter example in Figure 2.
- Type checking, assertions, root level access–are the code examples clean?
- Endpoints, especially legacy endpoints, multiple APIs–legacy access may run under older security standards without patches and updates, so plan ahead for their upgrade
- Cultural giveaways (we will talk more about this next)

There is a good example of how API information can be exploited by cutting and pasting tokens, courtesy of Laxman Muthiyah of thezerohack, a whitehat who received a $12,500 bug bounty for reporting this. From an attacker point of view, this shows that relentless attention to detail pays well—will your docs stand up to it?

Other attack examples are found in Table 1.

Is security already a consideration for your API? Research has shown it is not usually a priority. In an analysis paper by Murphy, Alliyu, Macvean, Kery, and Myers (2017), security came in eleventh out of 27 categories; Documentation was even lower at fifteenth.

Usually security only jumps up the agenda when things start to fail, although data protection legislation, such as GDPR, shows that people can take data security seriously. Not everybody, though: a U.K. Conservative Party 2018 conference app accidentally released all their MPs' phone numbers.

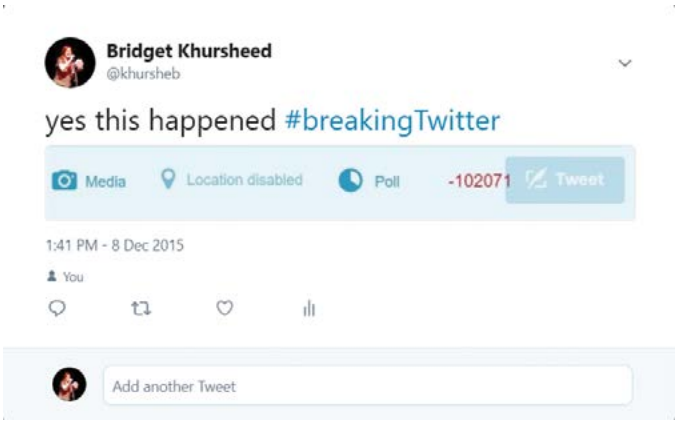


Figure 2: Breaking Twitter by adding undefined data; in this case, the results were humorous but in an API error, messages can give a lot away

Best Practices

So, security *is* on our agenda. Here's some things we can do immediately:

- For developers/security policy, include:
  - Writing restrictions like a least privilege policy
  - Secure authentication
  - Regular security audit/PEN test
- For API documentarians, include:
  - OPSEC obfuscation like hiding or disguising stuff
  - Abstraction (no examples from own company culture, multiple code examples, don't specify the source code language)
  - Hide data specifics where possible (no passwords obviously, but also pseudocode, obscure GETs examples, email format, etc.)
- For everyone:
  - Backup files (check for inappropriate content)
  - Watch out for features that train users to be less secure
  - Software error analysis

Attack Type	Target	Examples	Why It Matters
Social engineering	Social media, email, marketing materials	Phishing, geolocation, data gathering, observation see software tools like Echosec, The Harvester, Creepy (now a bit old but interesting) and the Iknowwhereyourcatlives.com project	Direct attacks but also information gathering to make attacks more successful; for example, local knowledge like when people arrive, where people go for lunch and names of colleagues helps a dial-in sound authentic if they are calling pretending to be from systems support
Spear phishing	Email, social media, etc.	Direct phishing usually aimed at a senior level person where good intel gathering beforehand is important to sound convincing	Ditto, but with higher rewards; often targets executive level with dramatic repercussions if successful
Software tools	Automated research prior to attack	Software to gather and manage information from APIs, available legitimately for pentesters or as Malware as a Service (MaaS)	Thriving marketplace via GitHub, Tor and discussion groups all make it possible to sort through vast amounts of data very quickly and often with the benefit of artificial intelligence (AI) and machine learning to increase effectiveness
Data gathering	OSINT	APIs, docs, knowledge base, social media channels trawled for information that is given away	Benign? But useful to competitors

Table 1. Attack types and why they matter

- Handle auto-generation with care
- Learn code
- Become cybersecurity aware (attend your local security meetup)
- Review standards like ISO 27001, NIST, and PCI-DSS
- Training in API security and social engineering

The good news is that security is a fun world to get involved in.

Conclusion: What You Can Do Next?

My main goal is to see technical communicators as an integral part of cybersecurity strategy and practice. My experience has shown that we have the skills, energy, and robust professionalism to communicate and ensure standards are met. How you proceed depends a little on where you sit, but here are three possibilities:

1. I would recommend that documentation managers locate their Corporate Information Security Policy (CISP) immediately and take a long hard look at it (if you haven't already done this).
2. Make yourself part of the security conversation over the whole company and develop explicit documentation security strategy. For communicators, be scrupulous—you may yourself be a target as you may have unusual access levels to code; avoid giving too much away via your personal channels and follow documentation best practices.
3. Finally, a note on freelancers or if you work remotely as this now has become the norm: Create your own CISP (there are templates available and you can perform a regular security audit of your systems and monitor risk, such as with email).

Let's start building a more secure world!

BRIDGET KHURSHEED *(poetandgeek @gmail.com) works as global documentation manager in a leading fintech. Her paper, "Microtargeting or Microphishing? Phishing Unveiled," is published in Trust, Privacy and Security in Digital Business 17th International Conference, TrustBus 2020, Bratislava, Slovakia, September 14-17, 2020 (Springer). She is also an award-winning poet and spoken word performer.*

REFERENCES

BBC News. 2018. "Conservative Party Conference app Reveals MPs' Numbers." Accessed 22 May 2021. *https://www.bbc.co.uk/news/uk-politics-45693143.*

Ferbrache, David. n.d. "Rise of Ransomware During COVID-19: How to Adapt to the New Threat Environment." KPMG. Accessed 21 May 2021. *https://home.kpmg/xx/en/home/insights/2020/05/rise-of-ransomware-during-covid-19.html.*

Hovsmith, Skip. 2019. "Preventing Mobile App and API Abuse." OWASP AppSecCali (You Tube video). Accessed 21 May 2021. *https://www.youtube.com/watch?v=QEW2AnEhfjs.*

Murphy, Lauren and Alliyu, Tosin, et al. 2017. "Preliminary Analysis of REST API Style Guidelines." PLATEAU'17. Accessed 21 May 2021. *http://www.cs.cmu.edu/~NatProg/papers/API-Usability-Styleguides-PLATEAU2017.pdf.*

Muthiyah, Laxman. 2021. "Deleting Any Photo Albums – How I Hacked Your Facebook Photos." The Zero Hack. Accessed 21 May 2021. *https://thezerohack.com/how-i-hacked-your-facebook-photos.*

DISCOVER YOUR **NEXT OPPORTUNITY** THROUGH

STC's Career Center

Career coaching, resume writing assistance, confidential reference checking, and even online learning to strengthen your interviewing and job search performance, all in one place, specifically for technical communicators.

Special Corporate Member Advantage: **Get 14-day advance access to the newest employment opportunities**

Start your search at **careers.stc.org**

A Great Adventure:
WORKING AS A SECURITY AWARENESS PROFESSIONAL IN HIGHER EDUCATION

By BEN WOELK, CISSP, CPTC | *Associate Fellow, Past STC President*

I HAVE THE most wonderful job in the world.

As I look back on 17 years of work in the Information Security Office at the Rochester Institute of Technology (RIT), I'm amazed at my career trajectory and how much I've learned. I've been able to take my tech comm skill set, apply it to my daily work in cybersecurity, and use that skill set to make a measurable difference for my community. I'm involved in cybersecurity compliance initiatives (not the most wonderful job part), but the bulk of my work is in cybersecurity training and awareness—which can be truly rewarding as you enable your community to protect themselves from cyberattackers.

Over the course of my career, I've achieved a Certified Information Systems Security Professional (CISSP) certification, and have had the opportunity to give presentations, author articles, and even teach workshops about how to do security awareness in a higher education setting. I'm also adjunct faculty, currently teaching classes in Cyber Security Policy and Law, Technical Writing and Editing, and Introverts and Leadership. Yes, I get to impact students in three areas that I'm passionate about. I've had quite the leadership journey in these areas, but today we're talking about my career in cybersecurity.

How Did I Get Here?

I had neither formal training in technical communication nor in cybersecurity. The latter field simply didn't exist when I was in college. (Yes, we had computers.)

After leaving my doctoral program in history, I began working as a technical communicator through contract houses and alongside my spouse, Marilyn Woelk, at Words by Design. The engagement that had the most impact on me in both learning how to do technical communication and becoming self-directed (stepping up) was my work as a consultant to the Xerox Corporation, where I served as a communications manager for the Client Services Group during a time of rapid technological change. My role was to help manage users through the change.

After my Xerox engagement ended, one of my former Xerox colleagues became RIT's Information Security Officer. He asked me to join them as a temporary employee to help with security incident-related communications. What started as a six-month engagement turned into a 17-year career.

The role grew over time into developing a security awareness and training program, drafting and managing policies and procedures, consulting with internal customers, managing projects, and an increasing number of compliance requirements. Although I didn't have a formal technical background in information technology, computer science, or cybersecurity, I was able to grasp the technical complexities of cybersecurity and contextualize them so that my audiences understood them, applied them to their jobs, and reduced risk. I also took advantage of tuition benefits to earn an Advanced Certificate in Technical Information Design.

Every job has its headaches, but I value the ability to influence (and help protect) my community, work with colleagues across the world, and invest in students. I can't imagine a more fulfilling occupation.

What Are My Key Learnings on this Journey?

Successful security awareness is about changing the culture. This process isn't quick. We need to build into our communities the ability to make quick, accurate decisions when they need to make a security-related decision. We enable them to easily recognize phishing attempts, practice good security hygiene around passwords, understand how to travel safely, and the like. A key element in forming the right behaviors is to ensure we're providing a variety of training activities that cover a breadth of threats. It's not enough to just focus on preventing phishing, or business email compromise attacks. We need to create robust programs that provide a steady breeze that enables users to develop strong roots to recognize and resist attacks (Woelk, 2019 "Wind, Trees, and Security Awareness").

What's Different About Working in Higher Education?

Successful security awareness in higher education is about innovation and doing more with less. We work in a challenging environment where everyone is either using or creating the next best thing. We're also in an industry where mandating training is rare and getting our community members' attention is challenging, so our messaging has to be concise and attention-getting. We don't have robust corporate budgets, so we work to create new and innovative programs. The Chronicle of Higher Education featured innovative security awareness work done by Harvard University, Texas A&M University, and the Rochester Institute of Technology in Julianne Basinger's, "A Campus Culture of Cybersecurity."

This willingness to build collaborative solutions isn't unique to higher education, but it's certainly in the forefront. Through my involvement with EDUCAUSE and its Awareness and Training Working Group, I've learned how to apply and create effective security awareness practices, and work with many colleagues at other universities to build solutions that are effective and that are offered freely. The EDUCAUSE Cybersecurity Awareness Resource Library is available to all.

Core Competencies for Success

As part of a research study (Woelk, 2016, "The Successful Security Awareness Professional") conducted through EDUCAUSE among security awareness practitioners at various colleges and universities, we determined that effective security awareness practitioners should have:

- An understanding of basic information security concepts, but not to the level required for the CISSP
- The ability to apply basic technical communication principles, including audience analysis and the ability to manage technical information in ways that allow people to take action
- The ability to apply basic instructional design principles, including analysis of learning need and systematic development of instruction

As technical communicators, you'll recognize that these core competencies mirror our skill sets—an ability to learn technical subject matter and contextualize it for our audiences through communications and training materials.

I'll add the ability to be flexible and adapt to changing priorities. In cybersecurity, it's rare that we have a week that's not interrupted by an incident of some type. In higher education, it's also rare that projects follow a straight line from conception to execution.

For a primer of cybersecurity terms, consult Tonie Flores's *The Language of Cybersecurity.*

Consider a career as a security awareness professional. I hope that you find it as rewarding as I have.

BEN WOELK *(benwoelkstc@gmail.com) CISSP, CPTC Trainer, is an Associate Fellow and Past President of STC. Ben is the Information Security Office Program Manager (and adjunct faculty) at the Rochester Institute of Technology. He's developed a highly regarded security awareness program and is a frequent speaker and workshop presenter for higher education.*

REFERENCES

Basinger, Julianne. 2019. "A Campus Culture of Cybersecurity." *The Chronicle of Higher Education.* Accessed 8 May 2021. *https://library.educause.edu/resources/2019/3/a-campus-culture-of-cybersecurity.*

EDUCAUSE Cybersecurity Awareness Resource Library. Accessed 8 May 2021. *https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/toolkits/cybersecurity-awareness-resource-library.*

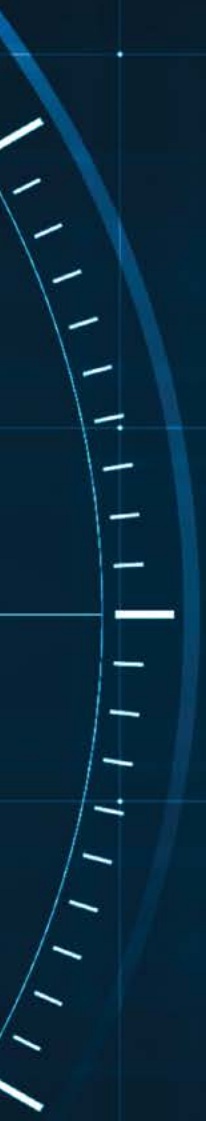
Flores, Marie Antonieta. 2018. *The Language of Cybersecurity.* XML Press.

Woelk, Ben. 2016. "Building a Culture of Digital Self Defense." *EDUCAUSE Review.* Accessed 8 May 2021. *https://er.educause.edu/blogs/2016/9/building-a-culture-of-digital-self-defense.*

Woelk, Ben. 2016. "The Successful Security Awareness Professional: Foundational Skills and Continuing Education Strategies." Educause. Accessed 8 May 2021. *https://library.educause.edu/resources/2016/8/the-successful-security-awareness-professional-foundational-skills-and-continuing-ed-strategies.*

Woelk, Ben. 2019. "We're All Winners--Gamification and Security Awareness." Slideshare. Accessed 8 May 2021. .*https://www.slideshare.net/bwoelk/were-all-winnersgamification-and-security-awareness*

Woelk, Ben. 2019. "Wind, Trees, and Security Awareness." *EDUCAUSE Review.* Accessed 8 May 2021. *https://er.educause.edu/blogs/2019/9/wind-trees-and-security-awareness*



A Short Career Sojourn into Cybersecurity

By DR. JACKIE DAMRAU | *STC Fellow*

CAREERS FOR SOME may span a single industry or go across multiple industries. The days of working for the same employer from early age to retirement age is no longer the norm (it's almost unheard of). Yet, as technical communicators, we know that the breadth of our field leads us in many directions.

My Cybersecurity Sojourn

My career started as a legal secretary followed by careers as a word processor, technical editor, instructional designer/trainer, business systems analyst, business process management analyst, with my next to last role being in cybersecurity.

In this article, I will share with you my 1–1/2-year cybersecurity sojourn as a Senior Risk Analyst/Senior Project Manager. I transitioned from a Senior Business Systems Analyst working on business process automation projects. This was fun, yet I accepted a challenge to transition to the Cybersecurity Governance, Risk, and Compliance (GRC) team. I knew nothing about cybersecurity at the time.

In my newly acquired role, I quickly put all my technical communication skills and experiences to practice. Soon I became the quality control point for all documentation leaving the team. I coached teammates on effective presentation skills, effective writing, and other basic skills we possess.

However, I learned from the folks that I was teaching about the subjects listed in Table 1.

> The world of cybersecurity will open your eyes to things you may not have paid much attention to before. It did for me.

My role also exposed me to international regulations like the General Data Privacy Regulation (GDPR) and the California Consumer Protection Act (CCPA). I learned that countries like Germany and France have Works Councils that require communications be passed through them for acceptance before rolling out to the employees. Even corporate policies that were of a global nature had to be presented and approved by the Works Councils; if not approved, then a separate policy had to be provided specifically for that country.

What's Needed for a Cybersecurity Career?

A technical communicator is not "just" a writer. We are editors, graphic designers, webmasters, business analysts, social media strategists, content strategists, instructional designers, procedure writers, and much more. According

Subject	Description
Data Content Stages	Structured/unstructured/semi-structured different than what technical communicators know
Data Classifications (Public, Confidential, Proprietary, Restricted)	Data tags or identifiers that classify the document by type, sensitivity, and value to the company. Use of these tags helps a company understand "the value of its data, determine whether the data is at risk, and implement controls to mitigate [these] risks" (Imperva, 2020). Effectively, data classifications help companies protect their "crown jewels" (most sensitive data) from leaving its doors and being used harmfully against the company.
Personal and Sensitive Data	Any data that can be used to identify you as a living being. When disparate pieces of information are put together, they can be traced back to a person. Hence, the bad actors use this information to steal your identity and do untoward things with it. There are more categories than one would know about, plus special categories that require protection for citizens in European Union countries. Visit my STC 2020 Technical Summit or LavaCon UX 2020 presentations for a thorough list of personal identifiers.
Password Protection	This is something we are constantly hearing about. You must have a different password for every website or business account that you have out in "Internetland." If you use built-in browser password managers, some professionals say that is not a good thing. The best protection is to use a password manager to randomly generate a complex password.
Data States (Data at Rest, Data in Transit, Data in Use)	Data states identify the different levels of protection needed on your data in its lifecycle. Here's brief definitions (Sealpath, 2020): **Data at Rest:** "Data that is not being accessed and is stored on a physical or logical medium (files stored on file servers, records in databases, documents on flash drives, hard disks, etc.)" **Data in Transit:** "Data that travels through an email, web, collaborative work applications [like] Slack or Microsoft Teams, instant messaging, or any type of private or public communication channel." **Data in Use:** Data that is "opened by one or more applications for its treatment and consumed or accessed by users."

Table 1. Subjects I learned from teammates I've coached

to RSI Security (2020), "A cybersecurity technical writer, or information security technical writer, creates written content for an organization in partial fulfillment of a comprehensive cybersecurity strategy.…The Bureau of Labor Statistics projects that demand for technical writers [in cybersecurity] will grow by 8 percent over the next several years." This means a new door is opening for technical communicators.

One can do a Google search for positions in cybersecurity and find that technical communicators are great candidates for these roles. Here's just a few to that you might consider looking into (SimplyHired, 2020):

- Cybersecurity Technical Writer
- Information Assurance Technical Writer
- Information Security Analyst / Technical Writer
- Policy/Procedure/Proposal Writers - Cybersecurity
- Security Analyst / Technical Writer
- Security Consultant Technical Writer

Skills or qualities one needs include:

- **Write documentation** for a specific purpose and specific audience on topics like "security policy, legal code, audit journaling, penetration test results, and business plans"
- **Detail-oriented** to spot high-level trends and significant anomalies with logical flow evidenced in the writing style
- **Comprehension of technical concepts** by learning "industry terms, understand[ing] causal relationships, and … distinguish[ing] relevant from irrelevant data"
- Determine **how much jargon or industry-specific terms** to use
- Play an active role as a **project manager or quality assurance person** for team documentation
- Willingness to **continuously learn new things** (the cybersecurity field constantly changes and requires knowing how to figure it out and move forward)

From roles, we move to certifications. It seems that almost every profession/career out there has some form of sanctioned certification body that adds acronyms after your name. Some of the more common ones in cybersecurity that technical communicators might consider are:

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- NIST Cybersecurity Framework (NCSF)
- Certified ISO 27001 ISMS Foundations/Lead Implementer/Lead Auditor
- Certified GDPR Practitioner

Cybersecurity is a new area for technical communication professionals to consider. There's lots of growth potential in this field.

Conclusion

The world of cybersecurity will open your eyes to things you may not have paid much attention to before. It did for me. I've given you a brief look into the world that I embraced, what skills/knowledge you need to be successful, and potential certifications/education you might consider. Enjoy your journey; reach out and let me know if you find it as exciting as I did.

Unfortunately, my company eliminated my position as a Senior Project Manager in November 2020. I was happy for the opportunity to learn a new industry and explore the opportunities that it gave me. I'm equally excited now to venture into my next role as a senior business analyst in the pharmaceuticals industry, another first for me.

DR. JACKIE DAMRAU (jdamrau3@gmail.com) is a Fellow of STC and the Book Review Editor of the Technical Communication journal. She is a senior business analyst with Carrollton Enterprise Services in New Orleans, Louisiana. Her former role was as a senior risk analyst/project manager for CBRE, Inc.

REFERENCES

Damrau, Jackie. 2020. "Structured and Unstructured Content: Perspectives from a Data Governance/Privacy Analyst." STC Technical Communication Summit 2020.

Damrau, Jackie. 2020. "Structured/Unstructured Content from a Data Protection View." LavaCon UX 2020.

Imperva. n.d. "Data Classification." Accessed 17 November 2020. *https://www.imperva.com/learn/data-security/data-classification/.*

RSI Security 2020. "What Makes a Great Cybersecurity Technical Writer?" Accessed 22 May 2021. *https://blog.rsisecurity.com/what-makes-a-great-cybersecurity-technical-writer/.*

Sealpath. 2020. "Protecting the three states of data." Accessed 22 May 2021. *https://www.sealpath.com/protecting-the-three-states-of-data/.*

SimplyHired. 2020. "20 Best Cyber Security Technical Writer Jobs (Hiring Now!)" Accessed 22 May 2021. *https://www.simplyhired.com/search?q=cyber+security+technical+writer&job=MFptGYiTwS5vyrrVTZoWhL-ar19xaEEnxicEqxtjOXOU6wpPETT3Ng.*

TC Authors Honored in Four Categories at 2021 CCCC Technical and Scientific Communication Awards

On Wednesday, 17 May, the Conference on College Composition & Communication presented its 2021 CCCC Awards in a live webinar, to recognize outstanding service, programs, publications, scholarship, and research.

Out of the six categories that the CCCC presents awards in for works in Technical and Scientific Communication, four of them recognized authors for their works in STC's *Technical Communication* journal.

The authors recognized were:

- **Edward A. Malone, David Wright, and Daniel Reardon** (Eds.), winners for "Best Original Collection of Essays in Technical or Scientific Communication."
- **Edward A. Malone** winner for "Best Article Reporting Historical Research or Textual Studies in Technical and Scientific Communication." "'Don't Be a Dilbert': Transmedia Storytelling as Technical Communication during and after World War II" in *Technical Communication*, 2019.
- **Josephine Walwema,** winner, for "A Values-Driven Approach to Technical Communication," in *Technical Communication*, 2020.
- **David Wright**, Honorable Mention, for "Best Article on Philosophy or Theory of Technical or Scientific Communication." "Sounding Off: Toward a Rhetoric of Sound in Technical Communication," in *Technical Communication*, 2019.

To be eligible for the awards, a nominee must be a member of CCCC and/or NCTE at the time of nomination. To nominate a work for the awards, the author, editor, publisher, or reader must be a CCCC and/or NCTE member.

For a complete list of award winners, go to: **https://cccc.ncte.org/cccc/awards/techsci.**

Searching for Your Next Tech Comm Dream Job?

STC PROVIDES ITS members with a robust Job Bank and Career Center where they can search for career opportunities with leading organizations from around the world. In addition to identifying career opportunities, members can access resources designed to help technical communicators at every stage of their careers. Post a resume, search the job listings, or create a personal job alert to let you know when jobs you want are available. This service is free to members.

Employers and recruiters can review resumes and post jobs. Visit the Job Bank page for pricing options and more to take advantage of the experience and skills gained by hiring STC members.

Access the STC Job Bank at:
https://careers.stc.org/

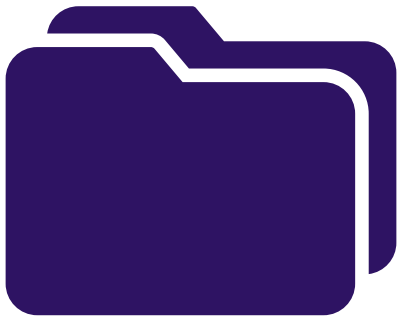
Looking for Technical Communication Academic Resources? Try the Academic Database!

LISA MELONÇON MAINTAINS a list of academic resources for technical communication.

From her site:

"*This project is a longitudinal study that has examined programs in technical and professional communication (TPC) over the last ~10 years. Gathering together what has become the most comprehensive data set ever collected, it focuses on a curricular view at the field-wide level by taking into account the field's curricular history as well as its current make-up. This project extends and updates some of my published research. More so, it brings together all the data into one place along with some practical tools for administrators and faculty who want to start, update, build, and/or sustain programs in TPC. These are a series of maps that display TPC degree programs at US institutions.*"

- For a full description of Lisa's methodology, see TechComm Programmatic Central.
- Explore the maps of US technical communication programs.



UPCOMING ONLINE COURSES

Online CPTC Preparatory Class

9 September to 28 October (Thursdays)
7:00 to 8:30 PM EST (GMT-4)

Registration closes 31 August 2021

THIS CLASS IS being offered through the Rochester Institute of Technology in conjunction with the STC Rochester Spectrum Conference.

In this eight-session class for certification, we will prepare you for the CPTC Foundation exam. Participants will learn the Nine Core Competency Areas for Technical Communicators that are evaluated by the Certified Professional Technical Communicator (CPTC) Foundation Exam. Subjects covered include project planning, project analysis, content development, organizational design, written communication, visual communication, reviewing and editing, content management, and production and delivery.

You're a Character: How Group Structure and Personality Types Influence Teamwork

Half-Day Workshop
Thursday, 9 September, 1:00 to 5:00 PM Eastern Time (GMT-4)

Registration closes 2 September 2021

PERSONALITY IS NOT an exact science. However, identifying your own personality traits helps you manage stress, identify triggers, and solve conflicts. Identifying traits of others helps you set teams, assign work, identify potential conflicts and plan mitigation, and solve interpersonal issues.

Register at **https://www.stc.org/education/online-courses/**

Get Certified!

HOW DO JOB seekers set themselves apart form the competition? With a CPTC certification!

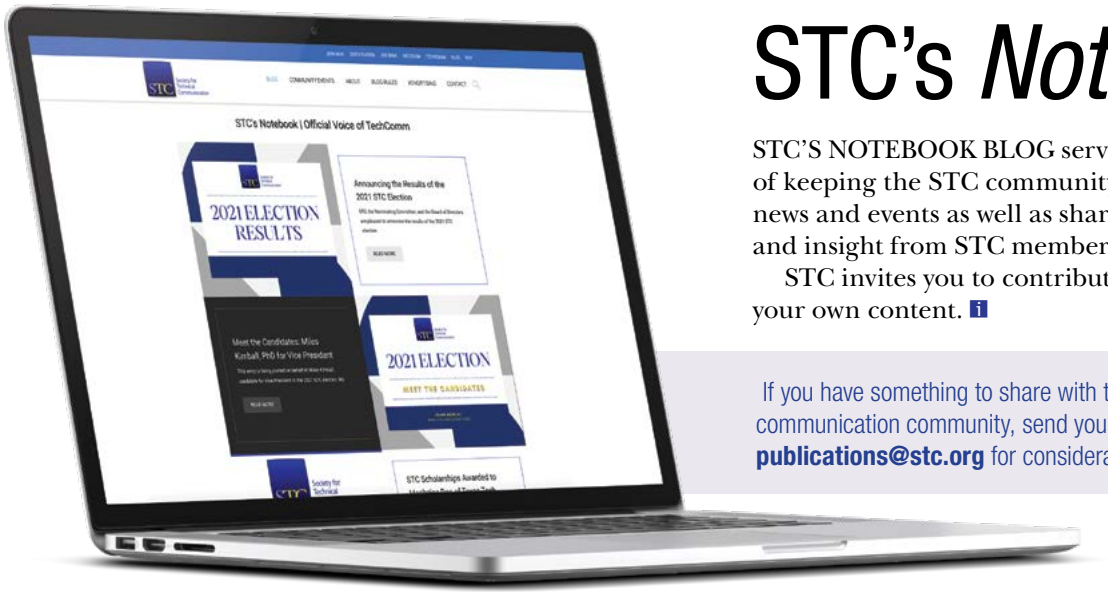
Professional certifications demand a robust understanding of the knowledge and specialized skills that are necessary to perform with a high degree of competence in a field. Additional annual requirements for training or practice ensure currency of skill and knowledge of new developments in that field. In every profession, professional certification helps employee, employer, and the consumer.

- The **Foundation** Certification focuses on knowledge of the field. To achieve the Certified Professional Technical Communicator (CPTC) – Foundational designation, applicants demonstrate knowledge and understanding of best practices in technical communication by passing a test. This is the first step in the CPTC ladder.
- The **Practitioner** Certification will demonstrate mastery of applying best practices and leading others in their use. The achievement of the Certified Professional Technical Communicator (CPTC)– Practitioner designation will be achieved by passing a test. Practitioner candidates must have Foundation Certification.
- Coming soon: The **Expert** Certification requirements will require a set of work products and expert interviews. (Those who achieved the Certified Professional Technical Communicator designation in 2012-2014 have been awarded the Certified Professional Technical Communicator Expert certification.)

Learn more at **www.stc.org/certification.**

"The CPTC certification was evidence that I had the credentials, and my active membership with STC was evidence that I was serious about my career. I got the job. My salary is $20,000 more than I was previously making and I have an office, not a cubicle with three walls, where my CPTC certificate prominently hangs."

-David Dick, STC Fellow


STC's Notebook | Official Voice of TechComm
2021 ELECTION RESULTS
Announcing the Results of the 2021 STC Election
2021 ELECTION
MEET THE CANDIDATES
STC Scholarships Awarded to

Contribute to STC's *Notebook*

STC'S NOTEBOOK BLOG serves an important role of keeping the STC community updated on Society news and events as well as sharing industry news and insight from STC members.

STC invites you to contribute to the blog with your own content.

If you have something to share with the technical communication community, send your submission to **publications@stc.org** for consideration.

Helping Eli Lilly Move to Adopt Structured Content for Customer Experience Improvements and Future Automation

BY SCOTT ABEL | *STC Associate Fellow*

THIS MONTH'S INSTALLMENT of "Meet the Change Agents" features my interview with John April, content strategy advisor at Eli Lilly and Company. April has agreed to share insights, lessons learned, and practical advice for teams planning to move from traditional desktop publishing-based content creation approaches to structured authoring.

SA: John, thanks for taking the time to speak with me about your experience moving to structured authoring. Your LinkedIn profile indicates you have deep experience helping your organization tackle all sorts of complex content challenges. Can you tell us a little bit about yourself—who you are, what you do, and why you do it?

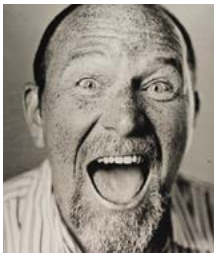
JA: I was trained to be a journalist. Over the past two decades, I've focused my skills on scientific communications supporting Lilly, mostly on regulatory content intended for study sites, regulatory bodies, or both. Nearly everyone I collaborate with is scientifically trained. In other circumstances, my input might not have been considered. But Lilly has leveraged my differences to help change the way it creates content.

I currently lead the implementation of structured authoring in Lilly's development organization. I also lead a team responsible for deploying content reuse software. The software will enable Lilly to increase its information integrity and realize time and cost savings. By making the content development process more efficient, I hope to honor and further Lilly's mission.

SA: When organizations understand the value of investing in structured content, it's often because they recognize the benefits of doing so can provide them. One of the main reasons why organizations start creating structured content is to develop new capabilities that will allow them to overcome impediments that prevent them from accomplishing business-critical work. Help our audience understand the conundrum facing your authoring team. What types of content-related challenges was your team facing?

JA: The initial challenge was to improve the user's experience with our content. The unstructured writing methods most of us were using didn't make the mental process of consuming content easy for our customers. Unstructured writing methods result in long, dense documents with repetitive content, important messages buried, numbers within copy that are difficult to interpret, parenthetical content that interrupts sentences, topic changes within a paragraph, different terms for the same concept, complex grammar, missing subjects, and other problems. These problems lead to a poor user experience where the customer wastes time reading and must re-read or ask questions about the content to understand it.

SA: I have found that selling the value of structured content to leaders usually involves more than



In the digital age, change happens quickly. This column features interviews with the movers and shakers—the folks behind new ideas, standards, methods, products, and amazing technologies that are changing the way we live and interact in our modern world. Got questions, suggestions, or feedback? Email them to *scott@thecontentwrangler.com.*

just convincing them to buy new software. Often, it requires helping them appreciate the capabilities that adopting structured content can provide their organizations. What capabilities are you aiming to develop by creating structured content?

JA: I advocated that the organization use structured authoring as a means not only to improve the user experience with our content, but also as a step of standardization necessary to achieve future automation. Structured content is not only easier for machines to consume but also to model, review for quality, translate, componentize, tag with metadata, associate with a unified taxonomy, repackage for multiple channels. In a word, structured content is easier to reuse.

SA: Moving to structured authoring is a change management issue as much as anything else. Can you talk a bit about the types of change challenges that our readers might face as they attempt to move their writers to a structured authoring environment?

JA: We started by training the organization's content development experts. At Lilly, these experts are medical writers. While medical writers are often scientifically trained, their primary expertise is the ability to write content well. Trainers must take these writers' skills apart and retool them so that their new reflex instinct is to adapt their writing to their audience's needs. I'd estimate it takes a good writer six to 12 months to become proficient in structured authoring. Once an organization's writing experts understand the methods and can advocate for their use, then you can begin to train people in other functions on the basics of structured authoring so they can better support the writers.

The biggest challenge in this transition is getting people who have been using unstructured writing methods all their lives to see the value in changing their ways. But isn't this the issue at the heart of all changes? Changes must be implemented in a certain order, and each person goes through the change at their own rate. First, you must make individuals aware of the problem or opportunity. Only once they have this awareness can they have the desire to participate in or support the change. Once they have the desire, the training effort is relatively straightforward. Most organizations won't have an in-house structured authoring trainer. Instead, they may leverage the vendor market's rich offerings. After training, constant reinforcement is necessary, so people adhere to the standard.

SA: When content teams adopt structured authoring, and they start practicing it daily, they almost always report experiencing a few a-ha moments—sudden realizations, inspirations, insights, recognitions, or comprehensions. Can you share with me one of your team's biggest a-ha moments?

JA: Once we began applying structured authoring methods, we saw massive page reductions in some of our documents. The content was much more useful and fit for purpose. People enjoyed reading the content because it was so consistently structured and easy for their brains to process.

SA: Common challenges can be difficult to avoid if you don't have someone to guide you toward content best practices and away from painful mistakes made by others who came before you. Did you bring in an external consultant to help your team develop your structured authoring program? If so, can you tell us a little about that experience and the benefits and drawbacks of working with an outside advisor?

JA: We hired a vendor specialized in structured authoring to design our training program and deliver it. The main drawback was their lack of expertise in our field. That resulted in the initial workshop being rather generic, particularly the training exercises, which focused on content our participants had no experience with. However, the benefit of using an experienced trainer far outweighed the drawbacks. Subsequent training workshops were easier for participants to consume because the vendor was willing to put in the time to work with us to tailor the training materials with our content.

SA: There's no shortage of best practices sessions at content conferences and online events. These types of sessions are popular with practitioners and usually provide some guidance on how to achieve success. It's also important to understand what not to do. Can you share any lessons learned from your adventures leading to the adoption of structured authoring?

JA: I think it's a good idea to train people on how to structure content before deploying a content management system.

Getting people to follow structured authoring methods in an authoring environment they're accustomed to, such as Word, might be a smoother ride than to try to introduce two big changes at the same time: change in writing method and change in the authoring environment.

SA: What books or other educational resources would you recommend to content teams who

are thinking about moving to structured authoring?

JA: Hire a structured authoring trainer who has codified their methods into a manual they give to workshop participants. That manual should always remain on the writer's desk and be their go-to resource on a day-to-day basis.

SA: Hindsight is, as they say, 20/20. If you could start your project all over again from scratch, knowing what you know now, would you do anything differently, and if so, what?

JA: Many of the concepts being offered by engineers of content management systems are not ready for scale, or organizations are not ready to scale with them. I would have performed more proof-of-concept testing and empathy sessions in my organization's current authoring environment to better understand the users' perspectives and needs. I also would have assembled a more comprehensive program strategy so that I had a clear roadmap showing me all the things I needed to change to ensure the project's success. Content strategists must change people's mindsets, and they can't do that overnight.

SA: We've talked a lot about structured authoring in this interview. Let's switch gears for a moment and chat about the most exciting thing you see in the world of information and knowledge management. What are you most excited about?

JA: I'm looking forward to more intuitive authoring systems that employ gamification principles to make the process of content development more fun. We need to expend more mental energy on design thinking and data interpretation and remove some of the stress that arises when we write. If reuse systems and automation tools could be more playful and approachable, I think people would be able to relax a bit at work and become more effective at their jobs.

SA: I want to thank you on behalf of our readers for taking time out of your schedule to share your insights, advice, and lessons learned about structured content. You've been very generous with your time, and I appreciate you sharing your expertise with our members. Thanks!

JA: Thank you for the chance to discuss these matters with you and address your readership.

CERTIFIED PROFESSIONAL
Technical Communicator
CPTC™
PRACTITIONER

PRACTITIONER CERTIFICATION

OPEN NOW

Certified Professional Technical Communicator™ (CPTC)

Be a leader. ***Have your Foundation Certification? Take your career to the next level by obtaining your Practitioner Certification.***

For more information about certification and to start the process, visit *www.stc.org* or email *stc@stc.org.*

Learn more at www.stc.org/certification

The Hidden Information Security Killers Hiding in Content, Metadata, and Operations

BY CRUCE SAUNDERS

SECURITY INCIDENTS RELATED to customer data have risen dramatically. Using data from the ITRC 2020 Data Breach Report, Statista.com found that "in 2020, the number of data breaches in the United States came in at a total of 1,001 cases. Over the course of the same year, over 155.8 million individuals were affected by data exposures...due to less-than-adequate information security."

The total economic impact of these breaches reaches into the billions of dollars, with the average breach costing $7.9 million.

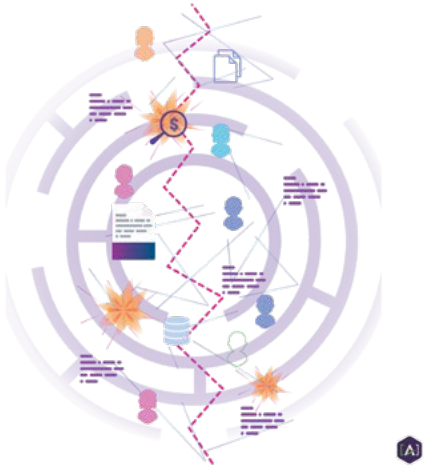


Figure 1. The impact of breaches

Organizations have a lot riding on security. So, what do content and metadata have to do with it?

There are hidden killers lurking in the content infrastructure of most organizations. If left unnoticed and unchecked, they are capable of inflicting enormous pain on an organization and its customers.

The Three Hidden Killers of Information Security

The least-noticed contributors to security breakdowns can be found in three important places:

1. The **policy** an organization maintains around content and data
2. The governance and **operations** structure around content
3. The **metadata** profile stored along with content items

If neglected, these hidden killers can leave open enormous vulnerability gaps and systemic issues that can cripple overall information security. But, if intentionally resourced and managed, these 'killers' can actually become contributors to security.

Modular Content, Modular Security

Content and data assets, even at the modular level, can and should store an understanding of what they are, where they come from, and who should consume them.

Security and permissions can be built in at the level of individual modules. Permission-based content targeting requires clear content access rights to be made available at the level of the content module. Security must tie into the content structures—specifically the metadata—of the content sets. Without functioning policy, operations, and controlled metadata information, security risk spreads across information sets. Breaches can then end up exposing untethered, non-policy-managed content and data assets to nefarious actors.

While data breaches have many causes, information security should consider the defensive hardness of the content assets themselves. Content leaders have a responsibility to ensure security from the assets on up.

The Cost of Unstructured Boundaries

Too often, a company's policies and procedures have grown into thick "how-to" instructions, originally in 3-ring shelfware–now evolved into fat PDF files, that are rarely remembered or consulted. This has partly stemmed from content governance being treated as a series of unpleasant, rigid rules.

Content creators may think they prefer a world with no rules in which they exercise unlimited creativity against a blank canvas. Alas, that free-spirited approach always comes with a cost.

In today's world of omnichannel content, drawn from many disparate sources (including partners and contractors), it's simply dangerous to ignore structures. As the systems and tools to create and collaborate increase our capabilities and sophistication, the need for safety guidelines and

Publishers face many challenges creating a new operating model and orchestration approach for dynamic omnichannel content. This column addresses the changing content ecosystem and the evolving dynamics in this space. Questions, suggestions, or feedback? Email *editorial@simplea.com*.

policies increases. But policies are not enough; they have to live and breathe in the content models, the infrastructure and tools, and in the day-to-day operations surrounding content.

Too often, organizations opt to ignore and absorb the risk and cost of continuing 'how we've always done it'. Unknowingly, the lack of governance leads to increases in:

- Regulatory risk and exposure
- Team frustration and lack of motivation
- Unclear responsibilities and processes
- Regulatory compliance negligence and fines
- Brand dilution
- Duplication of effort
- Lack of reuse
- Inconsistencies in quality

Rather than hemorrhaging these issues, content leaders are waking up to the benefits of a unified governance and operations approach. Within Content Operations engagements, [A] works with clients to design and implement a Content Orchestration Model (COM), that is engineered to enhance existing technology architectures, facilitates content creation efficiency, and provides policy adherence. Governance is not an afterthought; compliance is purposely designed early within the content supply chain so that creators can flourish within a pre-defined and constructed boundary.

Playing within Safe Boundaries

In [A]'s *Towards a Smarter World* podcast series, guest Kristina Podnar made some encouraging observations about end-user benefits with governance integrated into the content supply chain.

> "If you get the right policies, not only do you have velocity, but you have velocity in the right direction."

> "You tell your kids they can go play, they can do whatever they want to. They just can't leave the confines of your backyard and that fence. It's there to keep them safe. Now, they can do lots of crazy things. They can take the broom that's out there or the rake and they can pretend it's a horse. They can race worms like my child used to do. They can throw sand up in the air and pretend it's snowing."

> "But the reality is that they're safe in that backyard. We know they're not going to get run over by a car. We know nothing bad is going to happen to them. And when they're ready for dinner, they can come inside. And it's the same thing with policies. When you actually create policies, what you create for the organization, the enterprise for content creators or anybody else who is involved in digital is a nice, safe place where they can be creative, they can be innovative."

You can find even more insights in her book, *The Power of Digital Policy*.

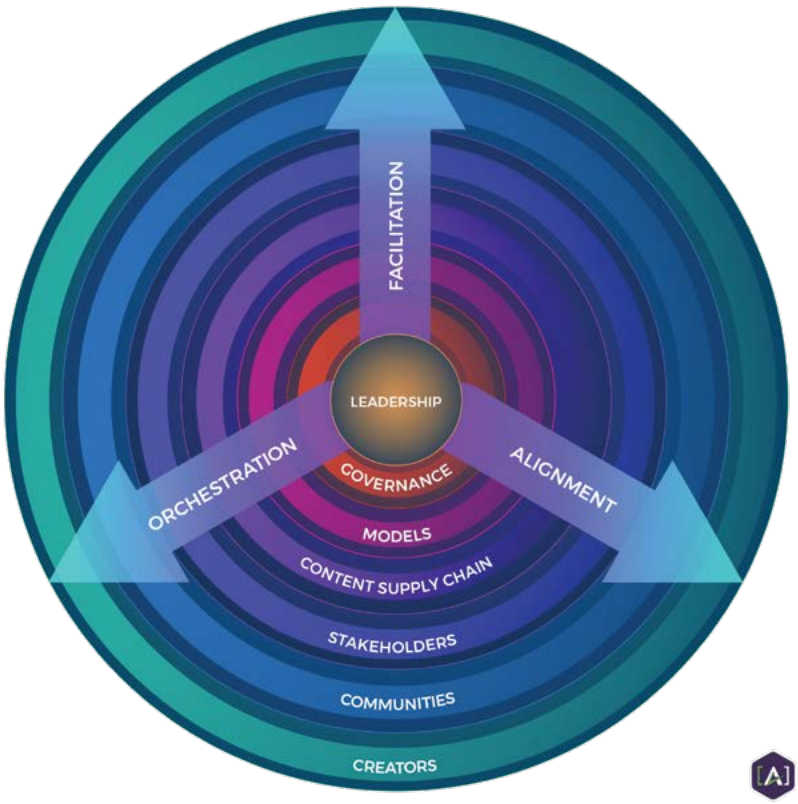


Figure 2. The Content Orchestration Model

Build Policy and Security Into Content Models

A key part of the security foundation can be built by implementing more thoughtful metadata procedures. We need to expand our content models with function-oriented elements that contain properties such as:

- Ownership
- Expiration
- Policies
- Regulations
- Read and Write Permissions
- Accessibility Variance
- Geographic Regulations
- Privacy Policy Variables

These content model elements, or metadata fields, provide the tremendous power of discrete controls and capacities to the content assets within a managed content supply chain. Rather than allowing the chaos of each department maintaining disparate metadata with no policy adherence, a Core Content Model is able to

unify and encompass a complete and shared metadata profile.

An added benefit of using [A]'s Core Content Model approach, is the ability to control and define mappings of content elements across channels and systems—the ability to perform nodal transformations.

Centralized Orchestration for Downstream Adherence and Efficiency

The most efficient content supply chains are run by a centralized, cross-functional Content Services Organization (CSO). This organization is composed of three separate practices: Content Strategy, Content Engineering, and Content Operations. To learn more about the CSO, see the referenced 2019 *Technical Communication* journal article, or visit simplea.com for additional resources. This can be coached and internally trained or driven by an integrated partner. In any form, it is needed.

Ensuring an optimized content supply chain for efficiency and compliance starts with a COM. It ties together policy considerations, business and publishing processes, defined content models, and stakeholder needs into a cleanly defined and "living" specification. It takes real orchestration, and that requires discovery and strategy before it happens. A Content Services Organization has dedicated staff to make sure that all aspects of content coordination work smoothly and are scalable.

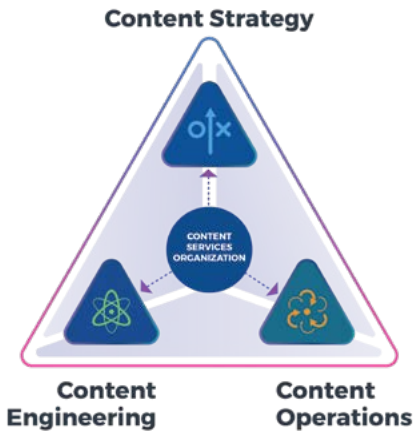


Figure 3. The Content Services Organization

5 Common Questions About Security

1. *How do we build content sets that are consistently aligned with an organization's regulatory and security mandates?*
   By baking security guidelines into the solution using policy, operations, and metadata, we can ensure consistency across company mandates.
2. *Who oversees and supports the security-aligned processes and procedures for creating content?*
   Processes are facilitated by a dedicated Content Operations function that references a written Content Orchestration Model, incorporating security standards.
3. *How do we automate security considerations into workflows?*
   Automation can be achieved by designing a content supply chain, enhanced by the security policies threaded into content sets using the disciplines and practices of content engineering.
4. *Where in the organization do policy-aligned and compliant content practices get defined?*
   Within an organizational-wide Content Services Organization (CSO) that oversees and addresses these issues, among others.
5. *How do we maintain security measures across all channels and platforms?*
   By expanding content models with permission metadata within content elements that are mapped, and able to transform for use, across systems and channels.

Information Security Starts at Home

The pain resulting from a lack of regulation and security can be very heavy. We've seen organizations in various industries struggle with finding material and wasting anywhere from 20-60 percent of their time manually transforming content from place to place or system to system. Not only is this costly in overhead, but these manual processes allow for more security risks to seep into procedures.

But all of that risk is avoidable with planning. Start with workshops that get the players into a common conversation. [A] hosts these, or they can be done internally. Yes, it does cost some money and time, but it is a lot less expensive to do things right up front than clean up after legal, regulatory, or security issues have gone wrong. It all starts with internal conversations, and then agreeing to get the house in order and secure.

With customer confidence and billions of dollars in direct and indirect costs on the line, the industry will benefit by revisiting and expanding the pivotal role of policy and its connection to engineering and operations across content teams.

REFERENCES

Identity Theft Resource Center. 2020. "15th Annual Data Breach Report." Accessed 22 May 2021. *https://notified.idtheftcenter.org/s/2020-data-breach-report.*

Podnar, Kristina. 2019. *The Power of Digital Policy: A Practical Guide to Minimizing Risk and Maximizing Opportunity for Your Organization*. NativeTrust Consulting, LLC.

Saunders, Cruce and Podnar, Kristina. 2020. "Digital Policy: Powering Operations, Innovation, and Velocity." Towards a Smarter World #20 (podcast).

Saunders, Cruce. 2019. "The Enterprise Content Services Organization." *Technical Communication* 66, no. 2: 163-176.

For more resources, visit simplea.com, *including our in-depth whitepapers introducing the Core Content Model and the Core Semantic Model.*

When Information Isn't Enough: Cybersecurity Scholarship and the Human Factor

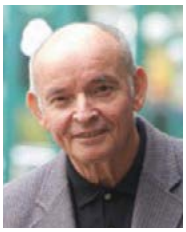
BY THOMAS BARKER | *STC Fellow*

IN AN ERA of international cyberattacks and social anxiety over data security, knowing where to start with communicative interventions can be a challenge. Technical communicators wishing to raise awareness of cybersecurity, increase stakeholder ownership of secure activities, and enhance user autonomy in threat mitigation need to take their words to the next level. These outcomes will quickly take the inexperienced communicator to the realization that *information isn't enough.*

In this article, we will turn to the academic conversation about cybersecurity and communication to see how researchers are exploring *and solving* the problem of stakeholder engagement in cybersecurity mitigation. We will look first at the communication situation: where do technical communicators fit into the big picture of cybersecurity communicative interventions. A look at communication skills for cybersecurity writing can help you identify learning resources. The next section will examine promising strategic—and persuasive—approaches like brain modeling. Finally, we will look at a few additional sources of investigation into communication modeling tools to get you out of a bind when you realize that *information isn't enough.*

Where Do Communicators Fit In?

The challenge facing communicators about cybersecurity issues are global and ubiquitous. I visited the Center for Strategic and International Studies to get a sense of the global nature of cybersecurity. High-profile attacks of government vs. government or government vs.



This column focuses on a broad range of practical academic issues from teaching and training to professional concerns, research, and technologies of interest to teachers, students, and researchers. Please send comments and suggestions to column editor Thomas Barker at *ttbarker@ualberta.ca.*

global trade groups are common, but abstract and irrelevant to most organizations. Closer to home, hacker groups practice targeting water supplies, creating fake Twitter and blog accounts, email phishing, and ransomware attacks. Take ransomware attacks alone: according to Mimecast.com, these occurred in six out of 10 companies. Email threats were also about that high. Almost 80 percent of organizations suffered from cyberattacks.

The role of technical communicators in cybersecurity is both external and internal. Externally, technical communicators need schooling in types of cybersecurity threats and organizational vulnerabilities to support data protection policies. The skill set for this work is complex, dynamic, and changing almost every day. Keeping up can be challenging, with a barrage of acronyms and hierarchical levels. To get a taste of this, check out Compliance Forge's Example Cybersecurity & Privacy Documentation. A good place to start might be the online training in the cybersecurity framework provided by the U.S. National Institute of Standards and Technology (NIST) Online Learning portal. Learn how to assess, profile, and plan your cybersecurity documentation initiatives. Want more? The NIST Computer Security Resource Center maintains an index of journal articles, white papers, conference papers, and books.

Internally, technical communicators and communication managers need to know at a basic level how to write audit reports, and at a larger level how to research, report on, communicate, develop, and staff security programs, assess security needs, communicate program design and training, and provide ongoing support and training. What's more, they need to work with cybersecurity professionals to learn their processes and solutions in order to convey that content to users.

Communication Skills

As a cybersecurity documentation specialist, you'll be working closely with individuals in other roles and departments, and it's important to be able to effectively communicate and explain your findings, concerns, and solutions to others. It's important to be able to speak clearly and concisely on cybersecurity strategy and policy, as well as to be able to convey technical information to individuals who possess different levels of technical comprehension.

The bottom line for cybersecurity writers is twofold: helping employees understand and follow cybersecurity best practices, and helping employees adopt a productive attitude towards these practices. A research paper on password policy by NIST insiders makes this point clearly: "Positive attitudes are related to more secure behaviors such as choosing stronger passwords and writing down passwords less often, less frustration with authentication procedures, and better understanding and respecting the significance of protecting passwords and system security." What this tells us is that with cybersecurity, as with so many other complex and detailed policies, users need more than just information; they need to know *why*. In these instances, words are not enough.

When words *are* enough, you can count on documentation of tools, formats, and examples of crafting of policy and assessment and audit reports to get you by. Here, again, the NIST can provide a number of tools and templates for privacy and security assessment, including use cases. Betterteam offers a host of templates for all sorts of cybersecurity policy documents, including policy, but also on cybersecurity topics that relate to social media use, remote work, cell phones, and other equipment. An even more informative list of employees' cybersecurity concerns (email, internet, encryption, anti-virus software, hardware, security breaches, and non-compliance) can be found at the FreePrivacyPolicy.com site.

But back to that problem that goes beyond information, when words fail to persuade. A 22-minute NPR story (see references below) can be your gateway into the science of persuasion. Why guess and stutter when you can use persuasion science! Good persuasion always starts with a problem, and works toward a solution. We read about this in Paul Anderson's textbook *Technical Communication: A Reader-Centered Approach,* which is easy to find on Google Books. Why trot out tired information about why people

The bottom line for cybersecurity writers is twofold: helping employees understand and follow cybersecurity best practices, and helping employees adopt a productive attitude towards these practices.

should protect passwords when all you have to do is suggest the dire consequences of not changing passwords?

Persuasion 101

Persuasive strategies like this, said expert Robert Cialdini, can turn attitudes about cybersecurity your way. The principle of encouraging users to be part of the correct choice and a unifying choice can sway attitudes. What does this mean for cybersecurity? The message may not be "protect your password" but "be a password protector." The shift here is subtle but powerful, because the second technique has the logic of social proof behind it. Additionally, prospect theory, the idea that loss framing can motivate, can also help employees internalize security behaviors, especially if those employees are prone to taking security risks. As a rule of thumb, gain-framing can work for risk-averse individuals (who, guess what, already make good decisions about security) but loss-framing can galvanize those risk-prone individuals who just don't see the danger of logging in to unsecure networks. The social norms theory approach can also work well in cybersecurity arguments, when the well-informed technical communicator can accurately show that most employees do, in fact, use safe cybersecurity behaviors. This technique can bring others on board.

The Academic Conversation about Cybersecurity

How important is the human factor in cybersecurity? Let's just ask the psychologists. Bruce Schneier, an early guru of cryptography, wrote: "Only amateurs attack machines. Professionals target people." They go for the soft target for a better return. Lillian Ablon, writing for Rand Corporation, puts it this way, "The human element is becoming increasingly prevalent in cyber and computer network operations—and is also the most unpredictable factor in cybersecurity." Most cyber attacks, it turns out, are not due to technical failures, but to human errors: the clicking on, opening up of, and entering onto phony accounts.

Considering the human element often means focusing on human behavior and its limitations. Alex Blau and his colleagues focus on this, showing how cognitive errors can creep. This occurs when users are updating software, responding to security warnings, and coding errors. *In Deep Thought: A Cybersecurity Story*, these psychologists suggest ways to help users make the right human decisions when faced with threats in these areas. For example, they show how users "go with their gut" in making bad decisions about downloading dangerous software: a cognitive shortcut known as the "affect heuristic."

My Brain Hurts!

In this article we looked briefly at the role of technical communicators in cybersecurity thinking and writing, both internally and externally. We looked at how the informative approach often gives way to a more strategic approach. Taking this path can point the content developer and policy writer to the real problem: people. The human element is where it's at in cybersecurity writing. So how to tap into the human brain for safer computing? The connection between technical communication and psychology has been documented by a number of researchers and academics. As Kai Weber notes, "Technical communication benefits greatly from cross-pollination with related disciplines, such as cognitive psychology." As we have seen in this article, technical communicators can use psychology and the human element to "think strategy" when words aren't enough.

REFERENCES

Betterteam. n.d. "Cyber Security Policy." Accessed June 11, 2021. *https://www.betterteam.com/cyber-security-policy.*

Blau, Alex, Alhadeff, Alexandra Stern, Michael, et al. *Deep Thought: A Cybersecurity Story.* New York, NY: Ideas42, 2017. *https://www.ideas42.org/wp-content/uploads/2016/08/Deep-Thought-A-Cybersecurity-Story.pdf.*

Center for Strategic and International Studies. n.d. "Significant Cyber Incidents." Accessed June 11, 2021. *https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.*

Compliance Forge. n.d. "Example Cybersecurity & Privacy Documentation." Accessed June 11, 2021. *https://www.complianceforge.com/example-cybersecurity-documentation.*

NIST. n.d "Online Learning Portal." Accessed June 11, 2021. *https://www.nist.gov/cyberframework/online-learning.*

NIST. n.d. "Risk Assessment Tools." Accessed June 11, 2021. *https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/collaboration-space/focus-areas/risk-assessment/tools.*

NIST. 2015. "What 4,500+ People Can Tell You: Employees' Attitudes Toward Organizational Password Policy Do Matter." Accessed June 11, 2021. *https://csrc.nist.gov/publications/detail/conference-paper/2015/08/02/what-4500-people-can-tell-you-employees-attitudes-password.*

NPR. 2008. "The Science of Getting A 'Yes.' " Accessed June 11, 2021. *https://www.npr.org/templates/story/story.php?storyId=93872977?storyId=93872977.*

Empowering Women Through Fiction

BY SHAWNEDA CROUT

I REMEMBER SITTING in the kitchen with my foster mom and her mother. We looked over my ten-year plan to graduate college and become a forensic psychologist for the FBI. Inspired by the books I'd read in middle school, I wanted to help the world by using my "natural ability to read people" to catch serial criminals. Once the cases were closed, I'd write books about them. Books like the ones I devoured in middle school.

Ten years later, I shipped my first Christian fiction novel and a poetry book to my foster dad. Sans the serial criminals, I'd written books using my "natural ability to read people" and extensive research to write medical fiction. These books helped the faith-based community discuss health issues like how to support believers diagnosed with HIV, obesity, and breast cancer. For five years, I lived beyond my childhood dreams as a full-time author.

The publishing landscape and industry shifted just as my personal life changed. I quickly realized that the social media and marketing skills I honed as an independent author were transferable skills. I'd gone from dreamer to author to marketing professional. What happens to a dream achieved?

For me, the dream achieved led to returning to school to study business, marketing, and technical communication. Learning about business and marketing showed me how to shift from dreaming to defining objectives and setting goals. The concepts and technologies I learned while studying technical communication sparked ideas for expanding my books into audio and visual content. A young bookworm's dream to become an author metamorphosed into a business-minded bookblerd's goal to translate her books into more mediums.

More personal life changes interrupted launching a new series in a new genre. Racial tensions and social unrest filled my workday as a social media and community manager for a hosting company. I struggled to find the creative space and energy to work on my books. From Twitter to LinkedIn, I couldn't escape the stories about the need to resolve problems caused by exclusion and inequities faced by African Americans. I wanted to help, but I know my strengths and weaknesses. I'm not built to dedicate my professional life to traditional corporate DEI work. So, I decided to support those doing the work. Life stepped in again.

Serendipitous events led to a reader showing me how to be a part of the solution as my tech writing, content creating, bookblerd self. The CROWN Act—Create a Respectful and Open World for Natural Hair—made headlines the exact same week my 2011 African American women's fiction book, *My Crowning Glory*, was featured on BookBub, a book discovery service. A BookBub reader who was not of African descent stated that she learned a lot by reading the book. Lightbulb moment! *My Crowning Glory* was written as an African American women's fiction series focused on natural hair, but it could provide insights for everyone.

Books shaped my empathy as a child. Reading about other ethnicities and cultures gave me an opportunity to choose to see them beyond their stereotypes and decide if they were as human as I am. As human as *I* hoped to be seen. Throughout my life, my circle has included women of all cultures, ethnicities, and backgrounds. So, I intentionally included women of all ethnicities in my Christian fiction series.

Fiction books welcome readers into worlds they may not know how to access. Books can be a safe way to see someone else's experience. To empathize and understand, we all have more in common than we may think. I'd already included women of all ethnicities in *Making Moves in Metropolis*, the first book of my new women's fiction series, the GiG PowHer series.

I write the GIG PowHer series and all the GIG PowHer Press series for readers who want to see beyond stereotypes. My new African American series in a new genre will continue to model new possibilities. Readers will find a fictional world focused on women who empower and celebrate each other. GIG PowHer Press books are how I help make the world a more inclusive and equitable place. My childhood self would be excited to know that future projects may even include a fictional serial criminal or two.

SHAWNEDA CROUT *(sc@shawneda.com) is a self-employed technical communicator with a Master of Arts degree in English, Technical Communication. When she's not creating solutions where technical communication merges with marketing you can find her doing low impact exercises with her daughter or publishing her books.*

Experience Professional Growth with STC Education!

STC offers a wide variety of online education options throughout the year. Whether you need an introduction to a subject, an in-depth review, or just a brush-up, STC has what you need. Advance your career with STC's varied collection of online education.

Live Weekly Webinars

Multi-Week Online Courses

Recorded Webinars

Free On-Demand Seminars
(Members Only)

Visit stc.org/education

CERTIFIED PROFESSIONAL

Technical Communicator

CPTC™

FOUNDATION

- **Project Planning**
- **Project Analysis**
- **Content Development**
- **Organizational Design**
- **Written Communication**
- **Reviewing & Editing**
- **Visual Communication**
- **Content Management**
- **Production & Delivery**

CONTACT

For more information about certification and to start the process, visit *www.stc.org* or email *stc@stc.org.*

Certified Professional Technical Communicator™ (CPTC)

Advance your Career and the Profession
Earn the CPTC Foundation Credential Today

The Certified Professional Technical Communicator (CPTC) credential assures employers, colleagues, and the public that you have the knowledge and skill to handle complex technical communication projects from the project planning stage through production and delivery.

Benefits

Why earn the CPTC credential? Because the CPTC credential:

- Distinguishes you from your peers;
- Shows you have the most up-to-date knowledge in the field;
- Opens up job opportunities and enhances job mobility;
- Elevates the profession;
- Gives you a sense of pride in your career; and
- Demonstrates your commitment to the field.

The CPTC credential gives you the edge you need to stand out to employers.

Continuing Education Requirements

Points may be obtained the following ways:

Event	Points
STC Annual Membership (any membership type for Foundation certificants)	2
STC Recorded Webinar (self-study)	1
STC Live Educational Webinar (free, sponsored, and community webinars excluded)	2
STC Online Courses	6
STC Summit Pre-Conference Courses (full day)	6
STC Summit Pre-Conference Courses (half day)	3
STC Annual Summit	8
Begin and complete a college-accredited course related to the Technical Communication field	8
Published articles that relate to any aspect of *Technical Communication* (2/article)	2
Published books publicly available on topics related to *Technical Communication* (5/book)	5
Presentations at conferences related to aspects of *Technical Communication* (2/presentation)	2
Total needed within 2 years post-certification date	**12**

Fees

Exam fees: STC Members $250, Non-Members, $495

Be a leader. ***Take your career to the next level by obtaining your credential. It's the most efficient way to prove your skills and knowledge in the technical communication field.***

Advance your Career and the Profession — Earn the CPTC Foundation Credential Today!
Learn more at www.stc.org/certification